



Council of the
European Union

190645/EU XXVII. GP
Eingelangt am 26/06/24

Brussels, 26 June 2024

10710/24

Interinstitutional File:
2021/0106 (COD)

JUR 266
TELECOM 204
JAI 947
COPEN 301
CYBER 184
DATAPROTECT 233
EJUSTICE 41
COSI 109
IXIM 151
ENFOPOL 279
RELEX 759
MI 576
COMPET 619
CODEC 1442

LEGISLATIVE ACTS AND OTHER INSTRUMENTS: CORRIGENDUM/RECTIFICATIF

Subject: Regulation (EU) of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828
(PE-CONS 24/1/24 REV 1, 14 June 2024)

LANGUAGES concerned: **ES, FR, HR, IT, NL, RO, SL**

PROCEDURE APPLICABLE (according to Council document R/2521/75):

— Procedure 2(b) (obvious errors in a number of language versions)

This text has also been transmitted to the European Parliament.

TIME LIMIT for the observations by Member States: 3 days

OBSERVATIONS to be notified to: dql.rectificatifs@consilium.europa.eu

(DQL RECTIFICATIFS (JUR 7), Directorate Quality of Legislation, Legal Service)

10710/24

JUR.7

EN

CORRECCIÓN DE ERRORES

del Reglamento del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

(PE-CONS 24/1/24 REV 1 de 14 de junio de 2024)

1) En la página 9, considerando 20, quinta frase:

donde dice:

«El Comité Europeo de Inteligencia Artificial (en lo sucesivo, «Comité») debe apoyar a la Comisión ...»,

debe decir:

«El Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA») debe apoyar a la Comisión ...».

- 2) En la página 50, considerando 53, última frase:
En la página 108, considerando 121, quinta frase:
En la página 128, considerando 143, tercera frase de la página 128 (undécima frase del considerando 143):
En la página 131, considerando 148, quinta frase:
En la página 132, considerando 149, primera, segunda, tercera, quinta (dos veces), sexta, novena y décima frases:
En la página 133, considerando 150, primera frase:
En la página 141, considerando 161, cuarta frase:

donde dice:

«Comité»,

debe decir:

«Consejo de IA».

- 3) En la página 180, artículo 6, apartado 5:

donde dice:

«5. La Comisión, previa consulta al Comité Europeo de Inteligencia Artificial (en lo sucesivo, «Comité»), y a más tardar el ...»,

debe decir:

«5. La Comisión, previa consulta al Consejo Europeo de Inteligencia Artificial (en lo sucesivo, «Consejo de IA»), y a más tardar el ...».

- 4) En la página 239, artículo 40, apartado 2, párrafo primero, última línea:
En la página 270, artículo 56, apartado 2, parte introductoria:
En la página 271, artículo 56, apartado 4, primera línea, y apartado 6, primera y segunda frases:
En la página 275, artículo 57, apartado 8, primera frase:
En la página 277, artículo 57, apartado 14, y apartado 15, primera frase:
En la página 278, artículo 57, apartado 16, primera frase:
En la página 293, artículo 62, apartado 3, letra a):

donde dice:

«Comité»,

debe decir:

«Consejo de IA».

- 5) En la página 295, artículo 65, título y apartado 1:

donde dice:

«Creación y estructura del Comité Europeo de Inteligencia Artificial

1. Se crea un Comité Europeo de Inteligencia Artificial (en lo sucesivo, “Comité”).»,

debe decir:

«Creación y estructura del Consejo Europeo de Inteligencia Artificial

1. Se crea un Consejo Europeo de Inteligencia Artificial (en lo sucesivo, “Consejo de IA”).».

- 6) En la página 296, artículo 65, apartado 2, primera, tercera y cuarta frases, apartado 4, parte introductoria y letras a), b) y c), y apartado 5, primera y segunda frases:
En la página 297, artículo 65, apartado 6, párrafos primero y tercero, apartado 7, y apartado 8, primera frase y segunda frase (dos veces):
En la página 298, artículo 66, título, parte introductoria, primera y segunda frases:
En la página 301, artículo 67, apartado 1:
En la página 302, artículo 67, apartado 8:
En la página 303, artículo 68, apartado 2, párrafo segundo:
En la página 308, artículo 70, apartado 6, última frase:
En la página 309, artículo 70, apartado 8, primera frase, y artículo 71, apartado 1, última frase:
En la página 321, artículo 75, apartado 2, penúltima línea:
En la página 336, artículo 84, apartado 2:
En la página 340, artículo 90, apartado 2, primera y segunda frases:
En la página 342, artículo 92, apartado 1, parte introductoria:
En la página 358, artículo 101, apartado 4:
En la página 372, artículo 112, apartado 8:
En la página 373, artículo 112, apartado 9:

donde dice:

«Comité»,

debe decir:

«Consejo de IA».

RECTIFICATIF

au règlement (UE) du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

(PE-CONS 24/1/24 REV 1 du 14 juin 2024)

Le texte du PE-CONS 24/1/24 REV 1 est remplacé par le texte suivant:

"RÈGLEMENT (UE) 2024/...
DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 juin 2024

**établissant des règles harmonisées concernant l'intelligence artificielle
et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013,
(UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE,
(UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)**

(Texte présentant de l'intérêt pour l'EEE)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,
vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,
vu la proposition de la Commission européenne,
après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen¹,

vu l'avis de la Banque centrale européenne²,

vu l'avis du Comité des régions³,

statuant conformément à la procédure législative ordinaire⁴,

¹ JO C 517 du 22.12.2021, p. 56.

² JO C 115 du 11.3.2022, p. 5.

³ JO C 97 du 28.2.2022, p. 60.

⁴ Position du Parlement européen du 13 mars 2024 (non encore parue au Journal officiel) et décision du Conseil du 21 mai 2024.

considérant ce qui suit:

- (1) L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle (ci-après dénommés "systèmes d'IA") dans l'Union, dans le respect des valeurs de l'Union, de promouvoir l'adoption de l'intelligence artificielle (IA) axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée "Charte"), y compris la démocratie, l'état de droit et la protection de l'environnement, de protéger contre les effets néfastes des systèmes d'IA dans l'Union, et de soutenir l'innovation. Le présent règlement garantit la libre circulation transfrontière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation de systèmes d'IA, sauf autorisation expresse du présent règlement.
- (2) Le présent règlement devrait être appliqué dans le respect des valeurs de l'Union consacrées dans la Charte, en facilitant la protection des personnes physiques, des entreprises, de la démocratie, de l'état de droit et de l'environnement, tout en stimulant l'innovation et l'emploi et en faisant de l'Union un acteur de premier plan dans l'adoption d'une IA digne de confiance.

- (3) Les systèmes d'IA peuvent être facilement déployés dans un large éventail de secteurs de l'économie et dans de nombreux pans de la société, y compris transfrontières, et peuvent facilement circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales destinées à faire en sorte que l'IA soit digne de confiance et sûre et à ce qu'elle soit développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Le fait que les règles nationales divergent peut entraîner une fragmentation du marché intérieur et peut réduire la sécurité juridique pour les opérateurs qui développent, importent ou utilisent des systèmes d'IA. Il convient donc de garantir un niveau de protection cohérent et élevé dans toute l'Union afin de parvenir à une IA digne de confiance, et d'éviter les divergences qui entravent la libre circulation, l'innovation, le déploiement et l'adoption des systèmes d'IA et des produits et services connexes au sein du marché intérieur, en établissant des obligations uniformes pour les opérateurs et en garantissant la protection uniforme des raisons impérieuses d'intérêt général et des droits des citoyens dans l'ensemble du marché intérieur sur la base de l'article 114 du traité sur le fonctionnement de l'Union européenne. Dans la mesure où le présent règlement contient des règles spécifiques sur la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel, à savoir des restrictions portant sur l'utilisation de systèmes d'IA pour l'identification biométrique à distance à des fins répressives, sur l'utilisation de systèmes d'IA pour l'évaluation des risques liés à des personnes physiques à des fins répressives, et sur l'utilisation de systèmes d'IA de catégorisation biométrique à des fins répressives, il convient de fonder le présent règlement, pour ce qui est de ces règles spécifiques, sur l'article 16 du traité sur le fonctionnement de l'Union européenne. Compte tenu de ces règles spécifiques et du recours à l'article 16 du traité sur le fonctionnement de l'Union européenne, il convient de consulter le comité européen de la protection des données.

- (4) L'IA est une famille de technologies en évolution rapide, contribuant à un large éventail de bienfaits économiques, environnementaux et sociétaux touchant l'ensemble des secteurs économiques et des activités sociales. En fournissant de meilleures prédictions, en optimisant les processus et l'allocation des ressources et en personnalisant les solutions numériques disponibles pour les particuliers et les organisations, le recours à l'IA peut donner des avantages concurrentiels décisifs aux entreprises et produire des résultats bénéfiques pour la société et l'environnement, dans des domaines tels que les soins de santé, l'agriculture, la sécurité des aliments, l'éducation et la formation, les médias, le sport, la culture, la gestion des infrastructures, l'énergie, les transports et la logistique, les services publics, la sécurité, la justice, l'utilisation efficace des ressources et de l'énergie, la surveillance de l'environnement, la préservation et la restauration de la biodiversité et des écosystèmes ainsi que l'atténuation du changement climatique et l'adaptation à celui-ci.
- (5) Cependant, en fonction des circonstances concernant son application et son utilisation et du niveau de développement technologique, l'IA peut générer des risques et porter atteinte aux intérêts publics et aux droits fondamentaux protégés par le droit de l'Union. Le préjudice causé peut être matériel ou immatériel, y compris physique, psychologique, sociétal ou économique.

- (6) Compte tenu de l'incidence majeure que l'IA peut avoir sur nos sociétés et de la nécessité de bâtir la confiance, l'IA et son cadre réglementaire doivent impérativement être élaborés dans le respect des valeurs de l'Union consacrées à l'article 2 du traité sur l'Union européenne, des droits et libertés fondamentaux prévus par les traités, et, conformément à l'article 6 du traité sur l'Union européenne, de la Charte. Il est indispensable que l'IA soit une technologie axée sur l'humain. Elle devrait servir d'outil aux personnes, dans le but ultime d'accroître le bien-être des humains.
- (7) Afin d'assurer un niveau cohérent et élevé de protection des intérêts publics en ce qui concerne la santé, la sécurité et les droits fondamentaux, il convient d'établir des règles communes pour les systèmes d'IA à haut risque. Ces règles devraient être conformes à la Charte, non discriminatoires et compatibles avec les engagements commerciaux internationaux de l'Union. Elles devraient également tenir compte de la déclaration européenne sur les droits et principes numériques pour la décennie numérique et des lignes directrices en matière d'éthique pour une IA digne de confiance rédigées par le groupe d'experts de haut niveau sur l'intelligence artificielle (ci-après dénommé "GEHN IA").

- (8) Un cadre juridique de l'Union établissant des règles harmonisées sur l'IA est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'IA dans le marché intérieur, tout en garantissant un niveau élevé de protection des intérêts publics, comme la santé et la sécurité, et de protection des droits fondamentaux, y compris la démocratie, l'état de droit et la protection de l'environnement, tels qu'ils sont reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, des règles régissant la mise sur le marché, la mise en service et l'utilisation de certains systèmes d'IA devraient être établies, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des marchandises et des services. Ces règles devraient être claires et solides pour protéger les droits fondamentaux, soutenir de nouvelles solutions innovantes, permettre la mise en place d'un écosystème européen d'acteurs publics et privés créant des systèmes d'IA conformes aux valeurs de l'Union, et libérer le potentiel de la transformation numérique dans l'ensemble des régions de l'Union. En établissant ces règles, ainsi que des mesures en faveur de l'innovation mettant un accent particulier sur les petites et moyennes entreprises (PME), parmi lesquelles les jeunes pousses, le présent règlement contribue à la réalisation de l'objectif qui consiste à promouvoir l'approche européenne de l'IA axée sur l'humain et faire de l'UE un acteur mondial de premier plan dans le développement d'une IA sûre, fiable et éthique, ainsi que l'avait formulé le Conseil européen⁵, et il garantit la protection de principes éthiques expressément demandée par le Parlement européen⁶.

⁵ Conseil européen, réunion extraordinaire du Conseil européen (1^{er} et 2 octobre 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

⁶ Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, 2020/2012 (INL).

- (9) Des règles harmonisées applicables à la mise sur le marché, à la mise en service et à l'utilisation de systèmes d'IA à haut risque devraient être établies conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil⁷, à la décision n° 768/2008/CE du Parlement européen et du Conseil⁸ et au règlement (UE) 2019/1020 du Parlement européen et du Conseil⁹ (ci-après dénommé "nouveau cadre législatif"). Les règles harmonisées énoncées dans le présent règlement devraient s'appliquer dans tous les secteurs et, conformément au nouveau cadre législatif, être sans préjudice du droit de l'Union en vigueur, en particulier en ce qui concerne la protection des données, la protection des consommateurs, les droits fondamentaux, l'emploi et la protection des travailleurs, et la sécurité des produits, que le présent règlement vient compléter. En conséquence, tous les droits et recours prévus par ce droit de l'Union pour les consommateurs et les autres personnes sur lesquelles les systèmes d'IA sont susceptibles d'avoir des incidences négatives, y compris en ce qui concerne la réparation de dommages éventuels conformément à la directive 85/374/CEE du Conseil¹⁰, demeurent inchangés et pleinement applicables.

⁷ Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) n° 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

⁸ Décision n° 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

⁹ Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) n° 765/2008 et (UE) n° 305/2011 (JO L 169 du 25.6.2019, p. 1).

¹⁰ Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux (JO L 210 du 7.8.1985, p. 29).

En outre, dans le contexte de l'emploi et de la protection des travailleurs, le présent règlement ne devrait donc pas avoir d'incidence sur le droit de l'Union en matière de politique sociale ni sur le droit national du travail, dans le respect du droit de l'Union, en ce qui concerne les conditions d'emploi et de travail, y compris la santé et la sécurité au travail et les relations entre employeurs et travailleurs. Par ailleurs, le présent règlement ne devrait pas porter atteinte à l'exercice des droits fondamentaux reconnus dans les États membres et au niveau de l'Union, notamment le droit ou la liberté de faire grève ou d'entreprendre d'autres actions prévues par les mécanismes de concertation sociale propres aux États membres, ainsi que le droit de négocier, de conclure et d'appliquer des conventions collectives ou de mener des actions collectives conformément au droit national. Le présent règlement ne devrait pas avoir d'incidence sur les dispositions visant à améliorer les conditions de travail dans le cadre du travail via une plateforme, établies dans la directive du Parlement européen et du Conseil relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme. De plus, le présent règlement vise à renforcer l'efficacité de ces droits et recours existants en établissant des exigences et des obligations spécifiques, y compris en ce qui concerne la transparence, la documentation technique et la tenue de registres des systèmes d'IA. Par ailleurs, les obligations imposées aux différents opérateurs intervenant dans la chaîne de valeur de l'IA en vertu du présent règlement devraient s'appliquer sans préjudice du droit national, dans le respect du droit de l'Union, ayant pour effet de limiter l'utilisation de certains systèmes d'IA lorsque ces législations ne relèvent pas du champ d'application du présent règlement ou poursuivent des objectifs légitimes d'intérêt public autres que ceux poursuivis par le présent règlement. Ainsi, le droit national du travail et les lois sur la protection des mineurs, à savoir des personnes âgées de moins de 18 ans, compte tenu de l'observation générale n° 25 (2021) de la CNUDE sur les droits de l'enfant en relation avec l'environnement numérique, dans la mesure où ils ne sont pas spécifiques aux systèmes d'IA et poursuivent d'autres objectifs légitimes d'intérêt public, ne devraient pas être affectés par le présent règlement.

- (10) Le droit fondamental à la protection des données à caractère personnel est garanti en particulier par les règlements (UE) 2016/679¹¹ et (UE) 2018/1725¹² du Parlement européen et du Conseil, ainsi que par la directive (UE) 2016/680 du Parlement européen et du Conseil¹³. Par ailleurs, la directive 2002/58/CE du Parlement européen et du Conseil¹⁴ protège la vie privée et la confidentialité des communications, y compris en prévoyant des conditions régissant le stockage de données à caractère personnel et non personnel dans des équipements terminaux ainsi que les conditions d'accès à ces données depuis ces équipements. Ces actes législatifs de l'Union servent de base à un traitement pérenne et responsable des données, y compris lorsque les ensembles de données contiennent un mélange de données à caractère personnel et de données à caractère non personnel. Le présent règlement n'entend pas modifier l'application du droit de l'Union régissant le traitement des données à caractère personnel, ni les tâches et les pouvoirs des autorités de contrôle indépendantes chargées de veiller au respect de ces instruments.

¹¹ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

¹² Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

¹³ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

¹⁴ Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

Il n'a pas non plus d'incidence sur les obligations des fournisseurs et des déployeurs de systèmes d'IA en leur qualité de responsables du traitement ou de sous-traitants découlant du droit de l'Union ou du droit national relatif à la protection des données à caractère personnel dans la mesure où la conception, le développement ou l'utilisation de systèmes d'IA implique le traitement de données à caractère personnel. Il convient également de préciser que les personnes concernées continuent de jouir de tous les droits et garanties qui leur sont conférés par le droit de l'Union, dont les droits liés à la prise de décision individuelle entièrement automatisée, y compris le profilage. Des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA établies en vertu du présent règlement devraient faciliter la mise en œuvre effective des droits et autres voies de recours garantis par le droit de l'Union relatif à la protection des données à caractère personnel et d'autres droits fondamentaux, et permettre aux personnes concernées de faire valoir ces droits et autres voies de recours.

- (11) Le présent règlement devrait être sans préjudice des dispositions relatives à la responsabilité des fournisseurs de services intermédiaires prévue dans le règlement (UE) 2022/2065 du Parlement européen et du Conseil¹⁵.

¹⁵ Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

- (12) La notion de "système d'IA" figurant dans le présent règlement devrait être clairement définie et devrait être étroitement alignée sur les travaux des organisations internationales œuvrant dans le domaine de l'IA afin de garantir la sécurité juridique, et de faciliter la convergence internationale et une large acceptation, tout en offrant la souplesse nécessaire pour tenir compte des évolutions technologiques rapides dans ce domaine. En outre, la définition devrait être fondée sur les caractéristiques essentielles des systèmes d'IA qui la distinguent des systèmes logiciels ou des approches de programmation traditionnels plus simples, et ne devrait pas couvrir les systèmes fondés sur les règles définies uniquement par les personnes physiques pour exécuter automatiquement des opérations. Une caractéristique essentielle des systèmes d'IA est leur capacité d'inférence. Cette capacité d'inférence concerne le processus consistant à générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions, qui peuvent influencer l'environnement physique ou virtuel, et la capacité des systèmes d'IA à inférer des modèles ou des algorithmes, ou les deux, à partir d'entrées ou de données. Les techniques permettant l'inférence lors de la construction d'un système d'IA comprennent des approches d'apprentissage automatique qui apprennent à partir des données la manière d'atteindre certains objectifs, et des approches fondées sur la logique et les connaissances qui font des inférences à partir des connaissances encodées ou de la représentation symbolique de la tâche à résoudre. La capacité d'un système d'IA à faire des inférences va au-delà du traitement de données de base en ce qu'elle permet l'apprentissage, le raisonnement ou la modélisation. Le terme "fondé sur des machines" renvoie au fait que les systèmes d'IA tournent sur des machines.

La référence à des objectifs explicites ou implicites souligne que les systèmes d'IA peuvent fonctionner selon des objectifs explicites définis ou des objectifs implicites. Les objectifs du système d'IA peuvent être différents de la destination du système d'IA dans un contexte spécifique. Aux fins du présent règlement, les environnements devraient s'entendre comme étant les contextes dans lesquels les systèmes d'IA fonctionnent, tandis que les sorties générées par le système d'IA correspondent à différentes fonctions exécutées par les systèmes d'IA et consistent en des prévisions, du contenu, des recommandations ou des décisions. Les systèmes d'IA sont conçus pour fonctionner à différents niveaux d'autonomie, ce qui signifie qu'ils bénéficient d'un certain degré d'indépendance dans leur action par rapport à une ingérence humaine et de capacités à fonctionner sans intervention humaine. La faculté d'adaptation dont un système d'IA pourrait faire preuve après son déploiement est liée à des capacités d'auto-apprentissage, qui permettent au système d'évoluer en cours d'utilisation. Les systèmes d'IA peuvent être utilisés seuls ou en tant que composant d'un produit, que le système soit physiquement incorporé dans le produit (intégré) ou qu'il serve la fonctionnalité du produit sans y être incorporé (non intégré).

- (13) Il convient d'interpréter la notion de "déployeur" visée dans le présent règlement comme désignant toute personne physique ou morale, y compris une autorité publique, une agence ou un autre organisme, utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel. En fonction du type de système d'IA, l'utilisation du système peut concerner des personnes autres que le déployeur.
- (14) Il convient d'interpréter la notion de "données biométriques" utilisée dans le présent règlement à la lumière de la notion de données biométriques au sens de l'article 4, point 14), du règlement (UE) 2016/679, de l'article 3, point 18), du règlement (UE) 2018/1725, et de l'article 3, point 13), de la directive (UE) 2016/680. Des données biométriques peuvent permettre l'authentification, l'identification ou la catégorisation des personnes physiques, ainsi que la reconnaissance de leurs émotions.
- (15) La notion d'"identification biométrique" visée dans le présent règlement devrait être définie comme la reconnaissance automatisée de caractéristiques physiques, physiologiques et comportementales d'une personne, telles que le visage, les mouvements oculaires, la forme du corps, la voix, la prosodie, la démarche, la posture, le rythme cardiaque, la pression sanguine, l'odeur et la frappe au clavier, aux fins d'établir l'identité d'une personne par comparaison des données biométriques de cette personne avec les données biométriques de personnes stockées dans une base de données de référence, que la personne ait donné son approbation ou non. En sont exclus les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, ce qui inclut l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux.

- (16) La notion de "catégorisation biométrique" visée dans le présent règlement devrait être définie comme le classement de personnes physiques dans certaines catégories sur la base de leurs données biométriques. Ces catégories spécifiques peuvent concerner des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits liés au comportement ou à la personnalité, la langue, la religion, l'appartenance à une minorité nationale ou encore l'orientation sexuelle ou politique. Cela n'inclut pas les systèmes de catégorisation biométrique qui sont une caractéristique purement accessoire intrinsèquement liée à un autre service commercial, ce qui signifie que cette caractéristique ne peut, pour des raisons techniques objectives, être utilisée sans le service principal, et l'intégration de cette caractéristique ou fonctionnalité n'est pas un moyen de contourner l'applicabilité des règles du présent règlement. Ainsi, les filtres de catégorisation des caractéristiques faciales ou corporelles qui sont utilisés sur les places de marché en ligne pourraient correspondre à ce type de caractéristique accessoire, étant donné qu'ils ne peuvent être utilisés qu'en lien avec le service principal, qui consiste à vendre un produit en permettant au consommateur d'afficher un aperçu du produit porté par lui-même et de l'aider à prendre une décision d'achat. Les filtres utilisés sur les services de réseaux sociaux en ligne qui classent par catégorie les caractéristiques faciales ou corporelles afin de permettre aux utilisateurs d'ajouter ou de modifier des images ou des vidéos pourraient également être considérés comme des fonctionnalités accessoires, étant donné que ce type de filtre ne peut pas être utilisé sans le service principal des services de réseau social consistant à partager des contenus en ligne.

- (17) La notion de "système d'identification biométrique à distance" visée dans le présent règlement devrait être définie, sur le plan fonctionnel, comme un système d'IA destiné à identifier des personnes physiques sans leur participation active, en règle générale à distance, par la comparaison des données biométriques d'une personne avec celles contenues dans une base de données de référence, quels que soient la technologie, les processus ou les types de données biométriques particuliers utilisés. Ces systèmes d'identification biométrique à distance sont généralement utilisés pour la perception simultanée de plusieurs personnes ou de leur comportement afin de faciliter sensiblement l'identification de personnes physiques sans leur participation active. Sont exclus les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, ce qui inclut l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux. Cette exclusion est justifiée par le fait que ces systèmes sont susceptibles d'avoir une incidence mineure sur les droits fondamentaux des personnes physiques par rapport aux systèmes d'identification biométrique à distance qui peuvent être utilisés pour le traitement des données biométriques d'un grand nombre de personnes sans leur participation active. Dans le cas des systèmes "en temps réel", la capture des données biométriques, la comparaison et l'identification se font toutes instantanément, quasi instantanément ou en tout état de cause sans décalage significatif. À cet égard, il convient, en prévoyant la possibilité de légers décalages, d'empêcher le contournement des règles du présent règlement relatives à l'utilisation "en temps réel" des systèmes d'IA concernés. Les systèmes "en temps réel" reposent sur l'utilisation d'éléments "en direct" ou "en léger différé", comme des séquences vidéo, générés par une caméra ou un autre appareil doté de fonctionnalités similaires. Dans le cas des systèmes "a posteriori", en revanche, les données biométriques sont prélevées dans un premier temps et la comparaison et l'identification n'ont lieu qu'après un délai substantiel. Cela suppose des éléments tels que des images ou des séquences vidéo, qui ont été générés par des caméras de télévision en circuit fermé ou des appareils privés avant l'utilisation du système à l'égard des personnes physiques concernées.

- (18) La notion de "système de reconnaissance des émotions" visée dans le présent règlement devrait être définie comme un système d'IA servant à identifier les émotions ou les intentions de personnes physiques ou à faire des déductions quant à leurs émotions ou intentions, sur la base de leurs données biométriques. Cette notion renvoie à des émotions ou des intentions telles que le bonheur, la tristesse, la colère, la surprise, le dégoût, la gêne, l'excitation, la honte, le mépris, la satisfaction et l'amusement. Cette notion ne recouvre pas les états physiques, tels que la douleur ou la fatigue, qui comprennent, par exemple, des systèmes utilisés pour déceler l'état de fatigue des pilotes ou des conducteurs professionnels aux fins de la prévention des accidents. Elle ne recouvre pas non plus la simple détection d'expressions, de gestes ou de mouvements dont l'apparence est immédiate, à moins que ceux-ci ne soient utilisés pour identifier ou déduire des émotions. Ces expressions peuvent être des expressions faciales toutes simples telles qu'un froncement de sourcils ou un sourire, ou des gestes tels qu'un mouvement de mains, de bras ou de tête, ou encore des caractéristiques de la voix d'une personne, comme le fait de parler fort ou de chuchoter.

- (19) Aux fins du présent règlement, la notion d'"espace accessible au public" devrait s'entendre comme désignant tout espace physique accessible à un nombre indéterminé de personnes physiques, que l'espace en question soit privé ou public, et indépendamment de l'activité pour laquelle il peut être utilisé, comme pour le commerce, par exemple, magasins, restaurants ou cafés, pour la prestation de services, par exemple, banques, activités professionnelles ou hôtellerie, pour la pratique de sports, par exemple, piscines, salles de sport ou stades, pour les transports, par exemple, gares routières, stations de métro et gares ferroviaires, aéroports ou moyens de transport, pour les divertissements, par exemple, cinémas, théâtres, musées, salles de concert et de conférence, ou pour les loisirs ou autres, par exemple, routes et places publiques, parcs, forêts ou terrains de jeux. Un espace devrait également être classé comme accessible au public si, indépendamment de la capacité potentielle ou des restrictions de sécurité, l'accès est soumis à certaines conditions prédéterminées qui peuvent être remplies par un nombre indéterminé de personnes, telles que l'achat d'un billet ou d'un titre de transport, l'enregistrement préalable ou le fait d'avoir un certain âge. En revanche, un espace ne devrait pas être considéré comme étant accessible au public si l'accès est limité à certaines personnes physiques, définies soit par le droit de l'Union soit par le droit national directement lié à la sûreté ou à la sécurité publiques, ou par la manifestation claire de la volonté de la personne disposant de l'autorité compétente sur l'espace. Le seul fait d'avoir une possibilité d'accès, comme une porte déverrouillée ou une porte ouverte dans une clôture, n'implique pas que l'espace est accessible au public en présence d'indications ou de circonstances suggérant le contraire, comme des signes d'interdiction ou de restriction d'accès. Les locaux des entreprises et des usines, ainsi que les bureaux et les lieux de travail qui sont destinés à être accessibles uniquement aux employés et prestataires de services concernés ne sont pas des espaces accessibles au public. Les espaces accessibles au public ne devraient pas inclure les prisons ni le contrôle aux frontières. D'autres espaces peuvent comprendre à la fois des espaces accessibles au public et des espaces non accessibles au public, comme le hall d'un bâtiment d'habitation privé par lequel il faut passer pour accéder au bureau d'un médecin ou le hall d'un aéroport. Les espaces en ligne ne sont pas couverts, car ce ne sont pas des espaces physiques. Le caractère accessible ou non au public d'un espace donné devrait cependant être déterminé au cas par cas, en tenant compte des particularités de la situation en question.

- (20) Afin de tirer le meilleur parti des systèmes d'IA tout en protégeant les droits fondamentaux, la santé et la sécurité et de permettre un contrôle démocratique, il convient que les fournisseurs, les déployeurs et les personnes concernées acquièrent, dans le cadre de la maîtrise de l'IA, les notions nécessaires pour prendre des décisions éclairées concernant les systèmes d'IA. Ces notions peuvent varier en fonction du contexte et peuvent recouvrir le fait de comprendre l'application correcte des éléments techniques au cours de la phase de développement du système d'IA, les mesures à appliquer pendant son utilisation, les moyens appropriés d'interpréter les sorties du système d'IA et, dans le cas des personnes concernées, les connaissances nécessaires pour comprendre comment les décisions prises avec l'aide de l'IA auront une incidence sur elles. Dans le cadre de l'application du présent règlement, la maîtrise de l'IA devrait fournir à tous les acteurs pertinents de la chaîne de valeur de l'IA les connaissances nécessaires pour en garantir le respect approprié et la mise en application correcte. En outre, la mise en œuvre à grande échelle de mesures relatives à la maîtrise de l'IA et l'introduction d'actions de suivi appropriées pourraient contribuer à améliorer les conditions de travail et, à terme, soutenir la consolidation et une trajectoire d'innovation d'une IA digne de confiance dans l'Union. Le Comité européen de l'intelligence artificielle (ci-après dénommé "Comité IA") devrait soutenir la Commission afin de promouvoir les outils de maîtrise de l'IA, la sensibilisation du public et la compréhension des avantages, des risques, des garanties, des droits et des obligations liés à l'utilisation des systèmes d'IA. En coopération avec les parties prenantes concernées, la Commission et les États membres devraient faciliter l'élaboration de codes de conduite volontaires au service de la maîtrise de l'IA chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA.

- (21) Afin de garantir des conditions de concurrence équitables et une protection efficace des droits et libertés des citoyens dans toute l'Union, les règles établies par le présent règlement devraient s'appliquer de manière non discriminatoire aux fournisseurs de systèmes d'IA, qu'ils soient établis dans l'Union ou dans un pays tiers, et aux déployeurs de systèmes d'IA établis dans l'Union.
- (22) Compte tenu de leur nature numérique, certains systèmes d'IA devraient relever du présent règlement même lorsqu'ils ne sont pas mis sur le marché, mis en service, ou utilisés dans l'Union. Cela devrait notamment être le cas lorsqu'un opérateur établi dans l'Union confie à un opérateur externe établi dans un pays tiers la tâche d'exécuter certains services ayant trait à une activité devant être réalisée par un système d'IA qui serait considéré comme étant à haut risque. Dans ces circonstances, le système d'IA utilisé dans un pays tiers par l'opérateur pourrait traiter des données légalement collectées et transférées depuis l'Union, et fournir à l'opérateur contractant établi dans l'Union les sorties dudit système d'IA provenant de ce traitement, sans que ce système d'IA soit mis sur le marché, mis en service ou utilisé dans l'Union. Afin d'éviter le contournement des règles du présent règlement et d'assurer une protection efficace des personnes physiques situées dans l'Union, le présent règlement devrait également s'appliquer aux fournisseurs et aux déployeurs de systèmes d'IA qui sont établis dans un pays tiers, dans la mesure les sorties produites par ces systèmes sont destinées à être utilisées dans l'Union.

Néanmoins, pour tenir compte des dispositions existantes et des besoins particuliers de coopération future avec les partenaires étrangers avec lesquels des informations et des preuves sont échangées, le présent règlement ne devrait pas s'appliquer aux autorités publiques d'un pays tiers ni aux organisations internationales lorsqu'elles agissent dans le cadre d'accords de coopération ou d'accords internationaux conclus au niveau de l'Union ou au niveau national pour la coopération des services répressifs et judiciaires avec l'Union ou avec les États membres, à condition que le pays tiers concerné ou les organisations internationales concernées fournissent des garanties adéquates en ce qui concerne la protection des libertés et droits fondamentaux des personnes. Le cas échéant, cela peut couvrir les activités des entités chargées par les pays tiers d'exécuter des tâches spécifiques à l'appui de cette coopération policière et judiciaire. De tels cadres de coopération ou accords ont été conclus bilatéralement entre des États membres et des pays tiers ou entre l'Union européenne, Europol et d'autres agences de l'Union, des pays tiers et des organisations internationales. Les autorités compétentes pour la surveillance des autorités répressives et judiciaires au titre du présent règlement devraient évaluer si ces cadres de coopération ou accords internationaux comportent des garanties adéquates en ce qui concerne la protection des libertés et droits fondamentaux des personnes. Les autorités nationales bénéficiaires et les institutions, organes et organismes de l'Union qui utilisent ces sorties dans l'Union demeurent responsables de veiller à ce que leur utilisation soit conforme au droit de l'Union. Lors de la révision de ces accords internationaux ou de la conclusion de nouveaux accords à l'avenir, les parties contractantes devraient tout mettre en œuvre pour aligner ces accords sur les exigences du présent règlement.

- (23) Le présent règlement devrait également s'appliquer aux institutions, organes et organismes de l'Union lorsqu'ils agissent en tant que fournisseurs ou déployeurs d'un système d'IA.

- (24) Si et dans la mesure où des systèmes d'IA sont mis sur le marché, mis en service ou utilisés avec ou sans modification de ces systèmes à des fins militaires, de défense ou de sécurité nationale, ces systèmes devraient être exclus du champ d'application du présent règlement, indépendamment du type d'entité exerçant ces activités, par exemple qu'il s'agisse d'une entité publique ou privée. En ce qui concerne l'usage à des fins militaires et de défense, une telle exclusion est justifiée tant par l'article 4, paragraphe 2, du traité sur l'Union européenne que par les spécificités de la politique de défense des États membres et de la politique de défense commune de l'Union relevant du titre V, chapitre 2, du traité sur l'Union européenne, qui sont soumises au droit international public, lequel constitue donc le cadre juridique le plus approprié pour la réglementation des systèmes d'IA dans le contexte de l'utilisation de la force létale et d'autres systèmes d'IA dans le cadre d'activités militaires et de défense. En ce qui concerne l'usage à des fins de sécurité nationale, l'exclusion est justifiée tant par le fait que la sécurité nationale reste de la seule responsabilité de chaque État membre, conformément à l'article 4, paragraphe 2, du traité sur l'Union européenne, que par la nature spécifique et les besoins opérationnels des activités liées à la sécurité nationale et par les règles nationales spécifiques applicables à ces activités. Néanmoins, si un système d'IA développé, mis sur le marché, mis en service ou utilisé à des fins militaires, de défense ou de sécurité nationale est, temporairement ou définitivement, utilisé en dehors de ce cadre à d'autres fins (par exemple, à des fins civiles ou humanitaires, à des fins répressives ou de sécurité publique), un tel système relèverait du champ d'application du présent règlement. Dans ce cas, l'entité qui utilise le système d'IA à des fins autres que militaires, de défense ou de sécurité nationale devrait veiller à la mise en conformité du système d'IA avec le présent règlement, à moins qu'il le soit déjà. Les systèmes d'IA mis sur le marché ou mis en service à des fins exclues, à savoir à des fins militaires, de défense ou de sécurité nationale, et à une ou plusieurs fins non exclues, comme à des fins civiles ou répressives, relèvent du champ d'application du présent règlement et les fournisseurs de ces systèmes devraient veiller au respect du présent règlement. En l'occurrence, le fait qu'un système d'IA puisse relever du champ d'application du présent règlement ne devrait pas affecter la possibilité pour les entités exerçant des activités de sécurité nationale, de défense et militaires, indépendamment du type d'entité exerçant ces activités, d'utiliser des systèmes d'IA à des fins de sécurité nationale, militaires et de défense, dont l'utilisation est exclue du champ d'application du présent règlement. Un système d'IA mis sur le marché à des fins civiles ou répressives qui est utilisé avec ou sans modification à des fins militaires, de défense ou de sécurité nationale ne devrait pas relever du champ d'application du présent règlement, indépendamment du type d'entité exerçant ces activités.

- (25) Le présent règlement devrait soutenir l'innovation et respecter la liberté scientifique et ne devrait pas compromettre les activités de recherche et de développement. Il est donc nécessaire d'exclure de son champ d'application les systèmes et modèles d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques. En outre, il est nécessaire de veiller à ce que le présent règlement n'affecte pas autrement les activités de recherche et de développement scientifiques relatives aux systèmes ou modèles d'IA avant leur mise sur le marché ou leur mise en service. En ce qui concerne les activités de recherche, d'essai et de développement axées sur les produits, relatives aux systèmes ou modèles d'IA, les dispositions du présent règlement ne devraient pas non plus s'appliquer avant la mise en service ou la mise sur le marché de ces systèmes et modèles. Cette exclusion est sans préjudice de l'obligation de se conformer au présent règlement lorsqu'un système d'IA relevant du champ d'application du présent règlement est mis sur le marché ou mis en service à la suite de cette activité de recherche et de développement, et sans préjudice de l'application des dispositions relatives aux bacs à sable réglementaires de l'IA et aux essais en conditions réelles. En outre, sans préjudice de l'exclusion des systèmes d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques, tout autre système d'IA susceptible d'être utilisé pour mener une activité de recherche et de développement devrait rester soumis aux dispositions du présent règlement. En tout état de cause, toute activité de recherche et de développement devrait être menée conformément à des normes éthiques et professionnelles reconnues en matière de recherche scientifique et dans le respect du droit de l'Union applicable.

- (26) Afin d'introduire un ensemble proportionné et efficace de règles contraignantes pour les systèmes d'IA, il convient de suivre une approche clairement définie fondée sur les risques. Cette approche devrait adapter le type et le contenu de ces règles à l'intensité et à la portée des risques que les systèmes d'IA peuvent générer. Il est donc nécessaire d'interdire certaines pratiques inacceptables en matière d'IA, de fixer des exigences pour les systèmes d'IA à haut risque et des obligations pour les opérateurs concernés, ainsi que de fixer des obligations de transparence pour certains systèmes d'IA.
- (27) Si l'approche fondée sur les risques constitue la base d'un ensemble proportionné et efficace de règles contraignantes, il importe de rappeler les lignes directrices en matière d'éthique pour une IA digne de confiance, élaborées en 2019 par le GEHN IA indépendant constitué par la Commission. Dans ces lignes directrices, le GEHN IA a élaboré sept principes éthiques non contraignants pour l'IA, qui sont destinés à contribuer à faire en sorte que l'IA soit digne de confiance et saine sur le plan éthique. Il s'agit des sept principes suivants: action humaine et contrôle humain; robustesse technique et sécurité; respect de la vie privée et gouvernance des données; transparence; diversité, non-discrimination et équité; bien-être sociétal et environnemental; et responsabilité. Sans préjudice des exigences juridiquement contraignantes du présent règlement et de toute autre disposition législative de l'Union applicable, ces lignes directrices contribuent à la conception d'une IA cohérente, fiable et axée sur l'humain, conformément à la Charte et aux valeurs sur lesquelles l'Union est fondée. Conformément aux lignes directrices du GEHN IA, "action humaine et contrôle humain" renvoient au fait que les systèmes d'IA sont développés et utilisés comme un outil au service des personnes, qui respecte la dignité humaine et l'autonomie de l'individu, et qui fonctionne de manière à pouvoir être contrôlé et supervisé par des êtres humains.

"Robustesse technique et sécurité" renvoient au fait que les systèmes d'IA sont développés et utilisés de manière à ce qu'ils soient techniquement robustes en cas de problème et résilients aux tentatives visant à en corrompre l'utilisation ou les performances afin de permettre à des tiers d'en faire une utilisation abusive, et à réduire le plus possible les atteintes involontaires. "Respect de la vie privée et gouvernance des données" renvoient au fait que les systèmes d'IA sont développés et utilisés conformément aux règles en matière de respect de la vie privée et de protection des données, dans le cadre d'un traitement de données répondant à des normes élevées en matière de qualité et d'intégrité.

"Transparence" renvoie au fait que les systèmes d'IA sont développés et utilisés de manière à permettre une traçabilité et une explicabilité appropriées, faisant en sorte que les personnes réalisent qu'elles communiquent ou interagissent avec un système d'IA, que les déployeurs soient dûment informés des capacités et des limites de ce système d'IA et que les personnes concernées soient informées de leurs droits. "Diversité, non-discrimination et équité" renvoient au fait que les systèmes d'IA sont développés et utilisés de manière à inclure des acteurs divers et à promouvoir l'égalité d'accès, l'égalité de genre et la diversité culturelle, tout en évitant les effets discriminatoires et les biais injustes, qui sont interdits par le droit de l'Union ou le droit national. "Bien-être sociétal et environnemental" renvoie au fait que les systèmes d'IA sont développés et utilisés d'une manière durable et respectueuse de l'environnement, mais aussi de manière à ce que tous les êtres humains en profitent, tout en surveillant et en évaluant les effets à long terme sur l'individu, la société et la démocratie. Ces principes devraient se retrouver, autant que possible, dans la conception et l'utilisation des modèles d'IA. Ils devraient en tout état de cause servir de base à l'élaboration de codes de conduite au titre du présent règlement. Toutes les parties prenantes, y compris l'industrie, le monde universitaire, la société civile et les organismes de normalisation, sont encouragées à tenir compte, ainsi qu'il convient, des principes éthiques pour l'élaboration de bonnes pratiques et de normes volontaires.

- (28) Si l'IA peut être utilisée à de nombreuses fins positives, elle peut aussi être utilisée à mauvais escient et fournir des outils nouveaux et puissants à l'appui de pratiques de manipulation, d'exploitation et de contrôle social. De telles pratiques sont particulièrement néfastes et abusives et devraient être interdites, car elles sont contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit, ainsi qu'aux droits fondamentaux consacrés dans la Charte, y compris le droit à la non-discrimination, le droit à la protection des données et à la vie privée et les droits de l'enfant.

- (29) Des techniques de manipulation fondées sur l'IA peuvent être utilisées pour persuader des personnes d'adopter des comportements indésirables ou pour les tromper en les poussant à prendre des décisions d'une manière qui met à mal et compromet leur autonomie, leur libre arbitre et leur liberté de choix. La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA ayant pour objectif ou pour effet d'altérer substantiellement les comportements humains, avec le risque de causer des dommages importants, en particulier d'avoir des incidences suffisamment importantes sur la santé physique ou psychologique ou sur les intérêts financiers, sont particulièrement dangereuses et devraient dès lors être interdites. Ces systèmes d'IA font intervenir des composants subliminaux, tels que des stimuli sonores, visuels ou vidéo que l'individu ne peut percevoir, étant donné que ces stimuli échappent à la perception humaine, ou d'autres techniques manipulatrices ou trompeuses qui mettent à mal ou altèrent l'autonomie de la personne, son libre arbitre ou sa liberté de choix de telle sorte que l'individu n'est pas conscient de ces techniques ou, à supposer qu'il le soit, sans qu'il puisse échapper à la duperie ni opposer une résistance ou un contrôle auxdites techniques. Cela pourrait être facilité, par exemple, par des interfaces cerveau-machine ou par la réalité virtuelle étant donné qu'elles permettent d'avoir plus de contrôle sur les stimuli qui sont présentés aux personnes, dans la mesure où elles peuvent en altérer sensiblement le comportement d'une manière très nocive. En outre, des systèmes d'IA peuvent également exploiter les vulnérabilités d'une personne ou d'un groupe particulier de personnes en raison de leur âge, d'un handicap au sens de la directive (UE) 2019/882 du Parlement européen et du Conseil¹⁶, ou d'une situation sociale ou économique spécifique susceptible de rendre ces personnes plus vulnérables à l'exploitation, telles que les personnes vivant dans une extrême pauvreté ou appartenant à des minorités ethniques ou religieuses.

¹⁶ Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

De tels systèmes d'IA peuvent être mis sur le marché, mis en service ou utilisés avec pour objectif ou pour effet d'altérer substantiellement le comportement d'une personne d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à une autre personne ou à des groupes de personnes, y compris des dommages susceptibles de s'accumuler au fil du temps, et il y a lieu, par conséquent, de les interdire. Il peut s'avérer impossible de présumer l'existence d'une intention d'altérer le comportement lorsque cette altération résulte de facteurs externes au système d'IA qui échappent au contrôle du fournisseur ou du déployeur, à savoir de facteurs qui ne peuvent être raisonnablement prévisibles, et partant, ne peuvent être atténués par le fournisseur ou le déployeur du système d'IA. En tout état de cause, il n'est pas nécessaire que le fournisseur ou le déployeur ait l'intention de causer un préjudice important, du moment que ce préjudice résulte de pratiques de manipulation ou d'exploitation reposant sur l'IA. Les interdictions de telles pratiques en matière d'IA complètent les dispositions de la directive 2005/29/CE du Parlement européen et du Conseil¹⁷, notamment concernant le fait que les pratiques commerciales déloyales entraînant des préjudices économiques ou financiers pour les consommateurs sont interdites en toutes circonstances, qu'elles soient mises en place au moyen de systèmes d'IA ou autrement. Les interdictions des pratiques de manipulation et d'exploitation prévues par le présent règlement ne devraient pas affecter les pratiques licites dans le cadre de traitements médicaux tels que le traitement psychologique d'une maladie mentale ou la rééducation physique, lorsque ces pratiques sont effectuées conformément à la législation applicable et aux normes médicales, comme le consentement explicite des personnes ou de leurs représentants légaux. En outre, les pratiques commerciales courantes et légitimes, par exemple dans le domaine de la publicité, qui respectent le droit applicable ne devraient pas, en soi, être considérées comme constituant des pratiques de manipulation préjudiciables reposant sur l'IA.

¹⁷ Directive n° 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil ("directive sur les pratiques commerciales déloyales") (JO L 149 du 11.6.2005, p. 22).

- (30) Il y a lieu d'interdire les systèmes de catégorisation biométrique fondés sur les données biométriques des personnes physiques, comme le visage ou les empreintes digitales, utilisés pour arriver à des déductions ou des inférences concernant les opinions politiques d'un individu, son affiliation à une organisation syndicale, ses convictions religieuses ou philosophiques, sa race, sa vie sexuelle ou son orientation sexuelle. Cette interdiction ne devrait pas couvrir l'étiquetage, le filtrage ou la catégorisation licites des ensembles de données biométriques acquis dans le respect du droit de l'Union ou du droit national en fonction de données biométriques, comme le tri des images en fonction de la couleur des cheveux ou de celle des yeux, qui peuvent par exemple être utilisés dans le domaine répressif.
- (31) Les systèmes d'IA permettant la notation sociale des personnes physiques par des acteurs publics ou privés peuvent conduire à des résultats discriminatoires et à l'exclusion de certains groupes. Ils peuvent porter atteinte au droit à la dignité et à la non-discrimination et sont contraires aux valeurs d'égalité et de justice. Ces systèmes d'IA évaluent ou classent les personnes physiques ou les groupes de personnes physiques en fonction de plusieurs points de données liées à leur comportement social dans divers contextes ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites pendant un certain temps. La note sociale obtenue à partir de ces systèmes d'IA peut conduire au traitement préjudiciable ou défavorable de personnes physiques ou de groupes entiers dans des contextes sociaux qui sont dissociés du contexte dans lequel les données ont été initialement générées ou collectées, ou à un traitement préjudiciable disproportionné ou injustifié au regard de la gravité de leur comportement social. Il y a donc lieu d'interdire les systèmes d'IA impliquant de telles pratiques de notation inacceptables et produisant de tels effets préjudiciables ou défavorables. Cette interdiction ne devrait pas avoir d'incidence sur les évaluations licites des personnes physiques qui sont pratiquées dans un but précis, dans le respect du droit de l'Union et du droit national.

- (32) L'utilisation de systèmes d'IA pour l'identification biométrique à distance "en temps réel" de personnes physiques dans des espaces accessibles au public à des fins répressives est particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux. Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Ce risque de résultats biaisés et d'effets discriminatoires est particulièrement significatif en ce qui concerne l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. En outre, du fait de l'immédiateté des effets et des possibilités limitées d'effectuer des vérifications ou des corrections supplémentaires, l'utilisation de systèmes fonctionnant en temps réel engendre des risques accrus pour les droits et les libertés des personnes concernées dans le cadre d'activités répressives ou affectées par celles-ci.

- (33) L'utilisation de ces systèmes à des fins répressives devrait donc être interdite, sauf dans des situations précisément répertoriées et rigoureusement définies, dans lesquelles l'utilisation se limite au strict nécessaire à la réalisation d'objectifs d'intérêt général dont l'importance l'emporte sur les risques encourus. Ces situations comprennent la recherche de certaines victimes d'actes criminels, y compris de personnes disparues; certaines menaces pour la vie ou la sécurité physique des personnes physiques, ou des menaces d'attaque terroriste; et la localisation ou l'identification des auteurs ou des suspects des infractions pénales énumérées dans une annexe du présent règlement, lorsque ces infractions pénales sont passibles, dans l'État membre concerné, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins quatre ans et telles qu'elles sont définies dans le droit dudit État membre. Le seuil fixé pour la peine ou la mesure de sûreté privative de liberté prévue par le droit national contribue à garantir que l'infraction soit suffisamment grave pour justifier l'utilisation de systèmes d'identification biométrique à distance "en temps réel". En outre, la liste des infractions pénales figurant en annexe du présent règlement sont basées sur les 32 infractions pénales énumérées dans la décision-cadre 2002/584/JAI du Conseil¹⁸, compte tenu du fait que certaines de ces infractions sont, en pratique, susceptibles d'être plus pertinentes que d'autres, dans le sens où le recours à l'identification biométrique à distance "en temps réel" pourrait, vraisemblablement, être nécessaire et proportionné, à des degrés très divers, pour les mesures pratiques de localisation ou d'identification d'un auteur ou d'un suspect de l'une des différentes infractions pénales répertoriées, eu égard également aux différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des éventuelles conséquences négatives.

¹⁸ Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

Une menace imminente pour la vie ou pour la sécurité physique des personnes physiques pourrait également résulter d'une grave perturbation d'une infrastructure critique, au sens de l'article 2, point 4), de la directive (UE) 2022/2557 du Parlement européen et du Conseil¹⁹, lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie ou la sécurité physique d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice de la fonction essentielle de l'État. Par ailleurs, le présent règlement devrait préserver la capacité des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile d'effectuer des contrôles d'identité en présence de la personne concernée conformément aux conditions prévues par le droit de l'Union et le droit national pour ces contrôles. En particulier, les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile devraient pouvoir utiliser des systèmes d'information, conformément au droit de l'Union ou au droit national, pour identifier une personne qui, lors d'un contrôle d'identité, soit refuse d'être identifiée, soit n'est pas en mesure de décliner son identité ou de la prouver, sans qu'il leur soit fait obligation par le présent règlement d'obtenir une autorisation préalable. Il peut s'agir, par exemple, d'une personne impliquée dans une infraction, qui ne veut pas ou ne peut pas divulguer son identité aux autorités répressives en raison d'un accident ou de son état de santé.

¹⁹ Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

- (34) Afin de s'assurer que ces systèmes soient utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune des situations précisément répertoriées et rigoureusement définies, certains éléments devraient être pris en considération, notamment en ce qui concerne la nature de la situation donnant lieu à la demande et les conséquences de l'utilisation pour les droits et les libertés de toutes les personnes concernées, ainsi que les garanties et les conditions associées à l'utilisation. En outre, l'utilisation, à des fins répressives, de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public ne devrait être déployée que pour confirmer l'identité de la personne spécifiquement ciblée et elle devrait être limitée au strict nécessaire dans le temps, ainsi que du point de vue de la portée géographique et personnelle, eu égard en particulier aux preuves ou aux indications concernant les menaces, les victimes ou les auteurs. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public ne devrait être autorisée que si l'autorité répressive compétente a réalisé une analyse d'impact sur les droits fondamentaux et, sauf disposition contraire du présent règlement, a enregistré le système dans la base de données prévue par le présent règlement. La base de données de référence des personnes devrait être appropriée pour chaque cas d'utilisation dans chacune des situations mentionnées ci-dessus.

- (35) Toute utilisation d'un système d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives devrait être subordonnée à l'autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre dont la décision est contraignante. Cette autorisation devrait en principe être obtenue avant l'utilisation du système d'IA en vue d'identifier une ou plusieurs personnes. Des exceptions à cette règle devraient être autorisées dans des situations dûment justifiées en raison du caractère urgent, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est de nature à rendre effectivement et objectivement impossible l'obtention d'une autorisation avant de commencer à utiliser le système d'IA. Dans de telles situations d'urgence, l'utilisation du système d'IA devrait être limitée au strict nécessaire et assortie de garanties et de conditions appropriées, telles qu'elles sont déterminées dans le droit national et spécifiées dans le contexte de chaque cas d'utilisation urgente par les autorités répressives elles-mêmes. En outre, l'autorité répressive devrait, dans ce genre de situation, solliciter une telle autorisation tout en indiquant les raisons pour lesquelles elle n'a pas été en mesure de le faire plus tôt, sans retard injustifié et au plus tard dans un délai de 24 heures. Lorsqu'une demande d'autorisation est rejetée, l'utilisation de systèmes d'identification biométrique en temps réel liés à cette autorisation devrait cesser immédiatement et toutes les données relatives à cette utilisation devraient être mises au rebut et supprimées. Ces données comprennent les données d'entrée directement acquises par un système d'IA au cours de l'utilisation de ce système, ainsi que les résultats et sorties de l'utilisation liée à cette autorisation. Cela ne devrait pas comprendre les entrées qui sont légalement acquises dans le respect d'un autre droit national ou du droit de l'Union. En tout état de cause, aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne devrait être prise sur la seule base des sorties du système d'identification biométrique à distance.

- (36) Afin de s'acquitter de leurs tâches conformément aux exigences énoncées dans le présent règlement ainsi que dans les règles nationales, l'autorité de surveillance du marché concernée et l'autorité nationale chargée de la protection des données devraient être informées de chaque utilisation du système d'identification biométrique en temps réel. Les autorités de surveillance du marché et les autorités nationales chargées de la protection des données auxquelles une notification a été adressée devraient présenter à la Commission un rapport annuel sur l'utilisation des systèmes d'identification biométrique en temps réel.
- (37) En outre, il convient de prévoir, dans le cadre exhaustif établi par le présent règlement, qu'une telle utilisation sur le territoire d'un État membre conformément au présent règlement ne devrait être possible que dans le cas et dans la mesure où l'État membre concerné a décidé de prévoir expressément la possibilité d'autoriser une telle utilisation dans des règles détaillées de son droit national. Par conséquent, les États membres restent libres, en vertu du présent règlement, de ne pas prévoir une telle possibilité, ou de prévoir une telle possibilité uniquement pour certains objectifs parmi ceux susceptibles de justifier l'utilisation autorisée définis dans le présent règlement. Ces règles nationales devraient être notifiées à la Commission dans les 30 jours suivant leur adoption.

- (38) L'utilisation de systèmes d'IA pour l'identification biométrique à distance en temps réel de personnes physiques dans des espaces accessibles au public à des fins répressives passe nécessairement par le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, et qui sont fondées sur l'article 16 du traité sur le fonctionnement de l'Union européenne, devraient s'appliquer en tant que *lex specialis* pour ce qui est des règles sur le traitement des données biométriques figurant à l'article 10 de la directive (UE) 2016/680, réglementant ainsi de manière exhaustive cette utilisation et le traitement des données biométriques qui en résulte. Par conséquent, une telle utilisation et un tel traitement ne devraient être possibles que dans la mesure où ils sont compatibles avec le cadre fixé par le présent règlement, sans qu'il soit possible pour les autorités compétentes, lorsqu'elles agissent à des fins répressives en dehors de ce cadre, d'utiliser ces systèmes et de traiter ces données pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement ne vise pas à fournir la base juridique pour le traitement des données à caractère personnel en vertu de l'article 8 de la directive (UE) 2016/680. Cependant, l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins autres que répressives, y compris par les autorités compétentes, ne devrait pas être couverte par le cadre spécifique concernant l'utilisation à des fins répressives établi par le présent règlement. L'utilisation à des fins autres que répressives ne devrait donc pas être subordonnée à l'exigence d'une autorisation au titre du présent règlement et des règles détaillées du droit national applicable susceptibles de donner effet à cette autorisation.

- (39) Tout traitement de données biométriques et d'autres données à caractère personnel mobilisées lors de l'utilisation de systèmes d'IA pour l'identification biométrique, qui n'est pas lié à l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, réglementée par le présent règlement, devrait rester conforme à toutes les exigences découlant de l'article 10 de la directive (UE) 2016/680. À des fins autres que répressives, l'article 9, paragraphe 1, du règlement (UE) 2016/679 et l'article 10, paragraphe 1, du règlement (UE) 2018/1725 interdisent le traitement de données biométriques sous réserve d'exceptions limitées prévues dans ces articles. En application de l'article 9, paragraphe 1, du règlement (UE) 2016/679, l'utilisation de l'identification biométrique à distance à des fins autres que répressives a déjà fait l'objet de décisions d'interdiction prises par les autorités nationales chargées de la protection des données.

- (40) Conformément à l'article 6 *bis* du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande n'est pas liée par les règles fixées à l'article 5, paragraphe 1, premier alinéa, point g), dans la mesure où il s'applique à l'utilisation de systèmes de catégorisation biométrique pour des activités dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, à l'article 5, paragraphe 1, premier alinéa, point d), dans la mesure où il s'applique à l'utilisation de systèmes d'IA couverts par cette disposition, à l'article 5, paragraphe 1, premier alinéa, point h), à l'article 5, paragraphes 2 à 6, et l'article 26, paragraphe 10, du présent règlement et adoptées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, lorsque l'Irlande n'est pas liée par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées.

- (41) Conformément aux articles 2 et 2 *bis* du protocole n° 22 sur la position du Danemark, annexé au traité l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par les règles fixées à l'article 5, paragraphe 1, premier alinéa, point g), dans la mesure où il s'applique à l'utilisation de systèmes de catégorisation biométrique pour des activités dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, à l'article 5, paragraphe 1, premier alinéa, point d), dans la mesure où il s'applique à l'utilisation de systèmes d'IA couverts par cette disposition, à l'article 5, paragraphe 1, premier alinéa, point h), à l'article 5, paragraphes 2 à 6, et à l'article 26, paragraphe 10, du présent règlement et adoptées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne, ni soumis à leur application, lorsqu'elles concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou du chapitre 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne.

- (42) Conformément à la présomption d'innocence, les personnes physiques dans l'Union devraient toujours être jugées sur leur comportement réel. Une personne physique ne devrait jamais être jugée sur la base d'un comportement prédit par l'IA uniquement sur la base de son profilage, de ses traits de personnalité ou de ses caractéristiques, telles que la nationalité, le lieu de naissance, le lieu de résidence, le nombre d'enfants, le niveau d'endettement ou le type de voiture, sans qu'il existe un motif raisonnable de soupçonner que cette personne est impliquée dans une activité criminelle sur la base de faits objectifs vérifiables et sans évaluation humaine de ceux-ci. Par conséquent, il convient d'interdire les évaluations des risques effectuées en ce qui concerne des personnes physiques dans le but d'évaluer la probabilité que ces dernières commettent une infraction ou de prévoir la survenance d'une infraction pénale, réelle ou potentielle, sur la seule base du profilage de ces personnes physiques ou de l'évaluation de leurs traits de personnalité et caractéristiques. En tout état de cause, cette interdiction ne vise ni ne concerne l'analyse des risques non fondée sur le profilage des personnes ou sur les traits de personnalité et les caractéristiques des individus, tels que les systèmes d'IA utilisant l'analyse des risques pour évaluer la probabilité de fraude financière de la part d'entreprises sur la base de transactions suspectes ou d'outils d'analyse des risques permettant de prédire la probabilité de la localisation de stupéfiants ou de marchandises illicites par les autorités douanières, par exemple sur la base de voies de trafic connues.
- (43) Il y a lieu d'interdire la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance, parce que cette pratique ne fait qu'accentuer le sentiment de surveillance de masse et peut entraîner des violations flagrantes des droits fondamentaux, y compris du droit au respect de la vie privée.

- (44) La base scientifique des systèmes d'IA visant à identifier ou à inférer les émotions suscite de vives inquiétudes, d'autant plus que l'expression des émotions varie considérablement d'une culture et d'une situation à l'autre, comme d'ailleurs chez un même individu. Les principaux défauts de ces systèmes sont, entre autres, leur fiabilité limitée, leur manque de précision et leur généralisabilité limitée. Par conséquent, les systèmes d'IA qui identifient ou déduisent les émotions ou les intentions de personnes physiques sur la base de leurs données biométriques peuvent conduire à des résultats discriminatoires et peuvent être intrusifs pour les droits et libertés des personnes concernées. Si l'on considère le déséquilibre de pouvoir qui existe dans le cadre du travail ou de l'enseignement, combiné au caractère intrusif de ces systèmes, ces derniers risqueraient de déboucher sur le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de personnes physiques. Par conséquent, il convient d'interdire la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA destinés à être utilisés pour déterminer l'état émotionnel de personnes physiques dans des situations liées au lieu de travail et à l'enseignement. Cette interdiction ne devrait pas porter sur les systèmes d'IA mis sur le marché strictement pour des raisons médicales ou de sécurité, tels que les systèmes destinés à un usage thérapeutique.
- (45) Le présent règlement devrait être sans effet sur les pratiques interdites par le droit de l'Union, notamment en vertu du droit de la protection des données, de la lutte contre la discrimination, de la protection des consommateurs et de la concurrence.

- (46) Les systèmes d'IA à haut risque ne devraient être mis sur le marché de l'Union, mis en service ou utilisés que s'ils satisfont à certaines exigences obligatoires. Ces exigences devraient garantir que les systèmes d'IA à haut risque disponibles dans l'Union ou dont les sorties sont utilisées d'une autre manière dans l'Union ne présentent pas de risques inacceptables pour d'importants intérêts publics de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union. Sur la base du nouveau cadre législatif, que la Commission a détaillé dans sa communication présentant le ""Guide bleu" relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022"²⁰, la règle générale est que plus d'un acte juridique de la législation d'harmonisation de l'Union, comme le règlement (UE) 2017/745²¹, le règlement (UE) 2017/746 du Parlement européen et du Conseil²² ou la directive 2006/42/CE du Parlement européen et du Conseil²³, peuvent s'appliquer à un produit dès lors que la mise à disposition ou la mise en service ne peut avoir lieu que lorsque le produit est conforme à l'ensemble de la législation d'harmonisation de l'Union applicable. Dans un souci de cohérence, et afin d'éviter des charges administratives ou des coûts inutiles, les fournisseurs d'un produit contenant un ou plusieurs systèmes d'IA à haut risque, auxquels s'appliquent les exigences du présent règlement et de la législation d'harmonisation de l'Union dont la liste figure en annexe du présent règlement, devraient disposer d'une certaine souplesse en ce qui concerne les décisions opérationnelles à prendre quant à la manière de garantir de façon optimale qu'un produit contenant un ou plusieurs systèmes d'IA est conforme à l'ensemble des exigences applicables de la législation d'harmonisation de l'Union. Les systèmes d'IA désignés comme étant à haut risque devraient être limités aux systèmes qui ont une incidence préjudiciable substantielle sur la santé, la sécurité et les droits fondamentaux des citoyens dans l'Union et une telle limitation devrait réduire au minimum toute éventuelle restriction au commerce international.

²⁰ JO C 247 du 29.6.2022, p. 1.

²¹ Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

²² Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

²³ Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24).

- (47) Les systèmes d'IA pourraient avoir un impact négatif sur la santé et la sécurité des citoyens, en particulier lorsque ces systèmes sont utilisés en tant que composants de sécurité de produits. Conformément aux objectifs de la législation d'harmonisation de l'Union visant à faciliter la libre circulation des produits sur le marché intérieur et à garantir que seuls des produits sûrs et conformes à d'autres égards soient mis sur le marché, il est important de dûment prévenir et atténuer les risques pour la sécurité susceptibles d'être créés par un produit dans son ensemble en raison de ses composants numériques, y compris les systèmes d'IA. Par exemple, des robots de plus en plus autonomes, que ce soit dans le secteur de l'industrie manufacturière ou des services de soins et d'aide à autrui, devraient pouvoir opérer et remplir leurs fonctions en toute sécurité dans des environnements complexes. De même, dans le secteur de la santé, où les enjeux pour la vie et la santé sont particulièrement importants, les systèmes de diagnostic de plus en plus sophistiqués et les systèmes soutenant les décisions humaines devraient être fiables et précis.

- (48) L'ampleur de l'incidence négative du système d'IA sur les droits fondamentaux protégés par la Charte est un critère particulièrement pertinent lorsqu'il s'agit de classer un système d'IA en tant que système à haut risque. Ces droits comprennent le droit à la dignité humaine, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'expression et d'information, la liberté de réunion et d'association, le droit à la non-discrimination, le droit à l'éducation, la protection des consommateurs, les droits des travailleurs, les droits des personnes handicapées, l'égalité de genre, les droits de propriété intellectuelle, le droit à un recours effectif et à accéder à un tribunal impartial, les droits de la défense et la présomption d'innocence, et le droit à une bonne administration. En plus de ces droits, il est important de souligner le fait que les enfants bénéficient de droits spécifiques consacrés à l'article 24 de la Charte et dans la convention des Nations unies relative aux droits de l'enfant (et précisés dans l'observation générale n° 25 de la CNUDE en ce qui concerne l'environnement numérique), et que ces deux textes considèrent la prise en compte des vulnérabilités des enfants et la fourniture d'une protection et de soins appropriés comme nécessaires au bien-être de l'enfant. Le droit fondamental à un niveau élevé de protection de l'environnement, consacré dans la Charte et mis en œuvre dans les politiques de l'Union, devrait également être pris en considération lors de l'évaluation de la gravité du préjudice qu'un système d'IA peut causer, notamment en ce qui concerne les conséquences pour la santé et la sécurité des personnes.

- (49) En ce qui concerne les systèmes d'IA à haut risque constituant des composants de sécurité de produits ou de systèmes, ou qui sont eux-mêmes des produits ou des systèmes entrant dans le champ d'application du règlement (CE) n° 300/2008 du Parlement européen et du Conseil²⁴, du règlement (UE) n° 167/2013 du Parlement européen et du Conseil²⁵, du règlement (UE) n° 168/2013 du Parlement européen et du Conseil²⁶, de la directive 2014/90/UE du Parlement européen et du Conseil²⁷, de la directive (UE) 2016/797 du Parlement européen et du Conseil²⁸,

²⁴ Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72).

²⁵ Règlement (UE) n° 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1).

²⁶ Règlement (UE) n° 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52).

²⁷ Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146).

²⁸ Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44).

du règlement (UE) 2018/858 du Parlement européen et du Conseil²⁹, du règlement (UE) 2018/1139 du Parlement européen et du Conseil³⁰ ou du règlement (UE) 2019/2144 du Parlement européen et du Conseil³¹, il convient de modifier ces actes pour veiller à ce que la Commission tienne compte, sur la base des spécificités techniques et réglementaires de chaque secteur, et sans interférer avec les mécanismes et les autorités de gouvernance, d'évaluation de la conformité et de contrôle de l'application déjà en place en vertu de ces règlements, des exigences obligatoires applicables aux systèmes d'IA à haut risque définis dans le présent règlement lors de l'adoption d'actes délégués ou d'actes d'exécution pertinents sur la base de ces actes.

²⁹ Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

³⁰ Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

³¹ Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

- (50) En ce qui concerne les systèmes d'IA qui constituent des composants de sécurité de produits relevant de certaines législations d'harmonisation de l'Union dont la liste figure en annexe du présent règlement, ou qui sont eux-mêmes de tels produits, il convient de les classer comme étant à haut risque au titre du présent règlement si le produit concerné est soumis à la procédure d'évaluation de la conformité par un organisme tiers d'évaluation de la conformité conformément à la législation d'harmonisation de l'Union correspondante. Ces produits sont notamment les machines, les jouets, les ascenseurs, les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles, les équipements radio, les équipements sous pression, les équipements pour bateaux de plaisance, les installations à câbles, les appareils brûlant des combustibles gazeux, les dispositifs médicaux, les dispositifs médicaux de diagnostic in vitro, l'automobile et l'aviation.
- (51) La classification d'un système d'IA comme étant à haut risque en application du présent règlement ne devrait pas nécessairement signifier que le produit utilisant le système d'IA en tant que composant de sécurité, ou que le système d'IA lui-même en tant que produit, est considéré comme étant à haut risque selon les critères établis dans la législation d'harmonisation de l'Union correspondante qui s'applique au produit en question. Tel est notamment le cas pour le règlement (UE) 2017/745 et le règlement (UE) 2017/746, dans le cadre desquels une évaluation de la conformité par un tiers est prévue pour les produits à risque moyen et les produits à haut risque.

- (52) En ce qui concerne les systèmes d'IA autonomes, à savoir les systèmes d'IA à haut risque autres que ceux qui constituent des composants de sécurité de produits ou qui sont eux-mêmes des produits, il convient de les classer comme étant à haut risque si, au vu de leur destination, ils présentent un risque élevé de causer un préjudice à la santé, à la sécurité ou aux droits fondamentaux des citoyens, en tenant compte à la fois de la gravité et de la probabilité du préjudice éventuel, et s'ils sont utilisés dans un certain nombre de domaines spécifiquement prédéfinis dans le présent règlement. La définition de ces systèmes est fondée sur la même méthode et les mêmes critères que ceux également envisagés pour toute modification ultérieure de la liste des systèmes d'IA à haut risque que la Commission devrait être habilitée à adopter, au moyen d'actes délégués, afin de tenir compte du rythme rapide de l'évolution technologique, ainsi que des changements potentiels dans l'utilisation des systèmes d'IA.

(53) Il importe également de préciser qu'il peut exister des cas spécifiques dans lesquels les systèmes d'IA visés dans des domaines prédéfinis spécifiés dans le présent règlement ne présentent pas un risque important d'atteinte aux intérêts juridiques protégés dans ces domaines parce qu'ils n'ont pas d'incidence substantielle sur la prise de décision ou ne causent pas de préjudice important à ces intérêts. Aux fins du présent règlement, il convient d'entendre par système d'IA qui n'a pas d'incidence substantielle sur le résultat de la prise de décision un système d'IA qui n'a pas d'incidence sur la substance et, partant, sur le résultat de la prise de décision, qu'elle soit humaine ou automatisée. Dans les cas où une ou plusieurs des conditions ci-après sont remplies, il pourrait s'agir d'un système d'IA qui n'a pas d'incidence substantielle sur le résultat de la prise de décision. La première de ces conditions devrait être que le système d'IA est destiné à accomplir une tâche procédurale étroite, comme transformer des données non structurées en données structurées, classer les documents entrants par catégories ou détecter les doublons parmi un grand nombre d'applications. Ces tâches sont par nature si étroites et limitées qu'elles ne présentent que des risques limités, qui ne sont pas exacerbés par une utilisation d'un système d'IA dans un contexte répertorié parmi les utilisations à haut risque dans la liste figurant en annexe du présent règlement. La deuxième condition devrait être que la tâche effectuée par le système d'IA est destinée à améliorer le résultat d'une activité humaine préalablement réalisée, susceptible d'être utile aux fins des utilisations à haut risque énumérées dans une annexe du présent règlement. Compte tenu de ces caractéristiques, le système d'IA n'ajoute qu'une couche supplémentaire à une activité humaine, ce qui présente par conséquent un risque réduit. Cette condition s'appliquerait par exemple aux systèmes d'IA destinés à améliorer la façon dont un document est rédigé, pour lui donner un ton professionnel ou un style académique ou pour l'adapter à un message de marque défini. La troisième condition devrait être que le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures.

Le risque serait réduit parce que l'utilisation du système d'IA intervient après la réalisation d'une évaluation humaine et n'est pas destinée à se substituer à celle-ci ni à l'influencer, sans examen humain approprié. Il s'agit par exemple des systèmes d'IA qui, compte tenu de certaines constantes habituelles observées chez un enseignant au niveau de la notation, peuvent être utilisés pour vérifier a posteriori si l'enseignant s'est éventuellement écarté de ces constantes, de manière à signaler d'éventuelles incohérences ou anomalies. La quatrième condition devrait être que le système d'IA est destiné à exécuter une tâche qui n'est qu'un acte préparatoire à une évaluation pertinente aux fins des systèmes d'IA repris dans la liste figurant dans une annexe du présent règlement et, partant, la probabilité que les sorties produites par le système présentent un risque pour l'évaluation postérieure est très faible. Cette condition s'applique, entre autres, aux solutions intelligentes de traitement des fichiers, qui comprennent diverses fonctions telles que l'indexation, la recherche, le traitement de texte et le traitement de la parole ou le fait de relier des données à d'autres sources de données, ou aux systèmes d'IA utilisés pour la traduction de documents initiaux. En tout état de cause, les systèmes d'IA utilisés dans des cas d'utilisation à haut risque énumérés dans une annexe du présent règlement devraient être considérés comme présentant des risques importants de préjudice pour la santé, la sécurité ou les droits fondamentaux si le système d'IA implique un profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679, de l'article 3, point 4), de la directive (UE) 2016/680 et de l'article 3, point 5), du règlement (UE) 2018/1725. Afin de garantir la traçabilité et la transparence, un fournisseur qui considère qu'un système d'IA n'est pas à haut risque sur la base des conditions susvisées devrait documenter l'évaluation avant la mise sur le marché ou la mise en service de ce système et fournir cette documentation aux autorités nationales compétentes sur demande. Ce fournisseur devrait être tenu d'enregistrer le système d'IA dans la base de données de l'UE établie en vertu du présent règlement. En vue de fournir des orientations supplémentaires pour la mise en œuvre pratique des critères en fonction desquels des systèmes d'IA répertoriés dans la liste figurant dans une annexe du présent règlement sont, à titre exceptionnel, des systèmes qui ne sont pas à haut risque, la Commission devrait, après consultation du Comité IA, fournir des lignes directrices précisant cette mise en œuvre pratique, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.

- (54) Étant donné que les données biométriques constituent une catégorie particulière de données à caractère personnel, il convient de classer comme étant à haut risque plusieurs cas d'utilisation critique des systèmes biométriques, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables. Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Le risque de tels résultats biaisés et d'effets discriminatoires est particulièrement important en ce qui concerne l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. Il convient par conséquent de classer les systèmes d'identification biométrique à distance comme étant à haut risque compte tenu des risques qu'ils présentent. Sont exclus de cette classification les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, parmi lesquelles l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux. En outre, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés pour la catégorisation biométrique en fonction d'attributs ou de caractéristiques sensibles protégés en vertu de l'article 9, paragraphe 1, du règlement (UE) 2016/679 sur la base de données biométriques, dans la mesure où ils ne sont pas interdits par le présent règlement, et les systèmes de reconnaissance des émotions qui ne sont pas interdits en vertu du présent règlement. Les systèmes biométriques destinés à être utilisés uniquement dans le but de permettre la cybersécurité et les mesures de protection des données à caractère personnel ne devraient pas être considérés comme des systèmes d'IA à haut risque.

- (55) En ce qui concerne la gestion et l'exploitation des infrastructures critiques, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans le cadre de la gestion et de l'exploitation des infrastructures numériques critiques visées à l'annexe I, point 8, de la directive (UE) 2022/2557, du trafic routier et de l'approvisionnement en eau, gaz, électricité et chauffage, car leur défaillance ou leur mauvais fonctionnement peut mettre en danger la vie et la santé de personnes à grande échelle et entraîner des perturbations importantes dans le déroulement normal des activités sociales et économiques. Les composants de sécurité des infrastructures critiques, y compris des infrastructures numériques critiques, sont des systèmes utilisés pour protéger directement l'intégrité physique des infrastructures critiques ou la santé et la sécurité des personnes et des biens, mais qui ne sont pas nécessaires au fonctionnement du système. La défaillance ou le mauvais fonctionnement de ces composants pourrait directement entraîner des risques pour l'intégrité physique des infrastructures critiques et, partant, des risques pour la santé et la sécurité des personnes et des biens. Les composants destinés à être utilisés uniquement à des fins de cybersécurité ne devraient pas être considérés comme des composants de sécurité. Les systèmes de surveillance de la pression de l'eau ou les systèmes de commande des alarmes incendie dans les centres d'informatique en nuage sont des exemples de composants de sécurité de ces infrastructures critiques.

- (56) Le déploiement de systèmes d'IA dans l'éducation est important pour promouvoir une éducation et une formation numériques de qualité et pour permettre à tous les apprenants et enseignants d'acquérir et de partager les aptitudes et compétences numériques nécessaires, y compris l'éducation aux médias, ainsi que l'esprit critique, pour participer activement à l'économie, à la société et aux processus démocratiques. Toutefois, les systèmes d'IA utilisés dans l'éducation ou la formation professionnelle, en particulier pour déterminer l'accès ou l'admission, pour affecter des personnes à des établissements ou programmes d'enseignement et de formation professionnelle à tous les niveaux, pour évaluer les acquis d'apprentissage des personnes, pour évaluer le niveau d'enseignement approprié d'une personne et influencer substantiellement le niveau d'enseignement et de formation dont bénéficiera cette personne ou auquel elle pourra avoir accès ou pour surveiller les étudiants au cours des épreuves et détecter les comportements interdits dans ce cadre devraient être classés comme étant à haut risque, car ils peuvent déterminer le parcours éducatif et professionnel d'une personne et peut par conséquent avoir une incidence sur la capacité de cette personne à assurer sa propre subsistance. Lorsqu'ils sont mal conçus et utilisés, ces systèmes peuvent être particulièrement intrusifs et mener à des violations du droit à l'éducation et à la formation ainsi que du droit à ne pas subir de discriminations, et perpétuer des schémas historiques de discrimination, par exemple à l'encontre des femmes, de certains groupes d'âge, des personnes handicapées ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle.

- (57) Les systèmes d'IA utilisés pour des questions liées à l'emploi, à la gestion de la main-d'œuvre et à l'accès à l'emploi indépendant, en particulier pour le recrutement et la sélection de personnes, pour la prise de décisions affectant les conditions des relations professionnelles, ainsi que la promotion et la résiliation des relations professionnelles contractuelles, pour l'attribution de tâches fondée sur le comportement individuel, les traits de personnalité ou les caractéristiques personnelles et pour le suivi ou l'évaluation des personnes dans le cadre de relations professionnelles contractuelles, devraient également être classés comme étant à haut risque car ces systèmes peuvent avoir une incidence considérable sur les perspectives de carrière et les moyens de subsistance de ces personnes ainsi que sur les droits des travailleurs. Les relations professionnelles contractuelles en question devraient concerner également, de manière significative, celles qui lient les employés et les personnes qui fournissent des services sur des plateformes telles que celles visées dans le programme de travail de la Commission pour 2021. Tout au long du processus de recrutement et lors de l'évaluation, de la promotion ou du maintien des personnes dans des relations professionnelles contractuelles, les systèmes d'IA peuvent perpétuer des schémas historiques de discrimination, par exemple à l'égard des femmes, de certains groupes d'âge et des personnes handicapées, ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle. Les systèmes d'IA utilisés pour surveiller les performances et le comportement de ces personnes peuvent aussi porter atteinte à leurs droits fondamentaux à la protection des données et à la vie privée.

- (58) Un autre domaine dans lequel l'utilisation des systèmes d'IA mérite une attention particulière est l'accès et le droit à certains services et prestations essentiels, publics et privés, devant permettre aux personnes de participer pleinement à la société ou d'améliorer leur niveau de vie. En particulier, les personnes physiques qui demandent à bénéficier ou bénéficient de prestations et services essentiels d'aide publique de la part des pouvoirs publics, à savoir des services de soins de santé, des prestations de sécurité sociale, des services sociaux fournissant une protection dans des cas tels que la maternité, la maladie, les accidents du travail, la dépendance ou la vieillesse et la perte d'emploi et l'aide sociale et au logement, sont généralement tributaires de ces prestations et services et se trouvent dans une situation vulnérable par rapport aux autorités compétentes. Lorsqu'ils sont utilisés pour déterminer si ces prestations et services devraient être accordés, refusés, réduits, révoqués ou récupérés par les autorités, y compris pour déterminer si les bénéficiaires y ont légitimement droit, les systèmes d'IA peuvent avoir une grande incidence sur les moyens de subsistance des personnes et porter atteinte à leurs droits fondamentaux, tels que le droit à la protection sociale, à la non-discrimination, à la dignité humaine ou à un recours effectif, et devraient donc être classés comme étant à haut risque. Néanmoins, le présent règlement ne devrait pas entraver la mise en place et l'utilisation, dans l'administration publique, d'approches innovantes qui bénéficieraient d'une utilisation plus large de systèmes d'IA conformes et sûrs, à condition que ces systèmes n'entraînent pas de risque élevé pour les personnes physiques et morales.

En outre, les systèmes d'IA utilisés pour évaluer la note de crédit ou la solvabilité des personnes physiques devraient être classés en tant que systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes à des ressources financières ou à des services essentiels tels que le logement, l'électricité et les services de télécommunication. Les systèmes d'IA utilisés à ces fins peuvent conduire à la discrimination entre personnes ou groupes et perpétuer des schémas historiques de discrimination, tels que ceux fondés sur les origines raciales ou ethniques, le sexe, les handicaps, l'âge ou l'orientation sexuelle, ou peuvent créer de nouvelles formes d'incidences discriminatoires. Toutefois, les systèmes d'IA prévus par le droit de l'Union aux fins de détecter les fraudes dans l'offre de services financiers et à des fins prudentielles pour calculer les besoins en fonds propres des établissements de crédit et des compagnies d'assurance ne devraient pas être considérés comme étant à haut risque au titre du présent règlement. Par ailleurs, les systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-santé et vie peuvent avoir une incidence significative sur les moyens de subsistance de ces personnes et, s'ils ne sont pas dûment conçus, développés et utilisés, peuvent porter atteinte à leurs droits fondamentaux et entraîner de graves conséquences pour leur vie et leur santé, y compris l'exclusion financière et la discrimination. Enfin, les systèmes d'IA utilisés pour évaluer et hiérarchiser les appels d'urgence émis par des personnes physiques ou pour envoyer des services d'intervention d'urgence ou établir des priorités dans l'envoi de tels services, y compris la police, les pompiers et les secours, ainsi que dans l'utilisation des systèmes de tri des patients admis dans les services de santé d'urgence, devraient aussi être classés comme étant à haut risque car ils prennent des décisions dans des situations très critiques pour la vie, la santé et les biens des personnes.

- (59) Compte tenu du rôle et de la responsabilité des autorités répressives, les actions menées par celles-ci qui supposent certaines utilisations de systèmes d'IA sont caractérisées par un degré important de déséquilibre des forces et peuvent conduire à la surveillance, à l'arrestation ou à la privation de la liberté d'une personne physique ainsi qu'à d'autres conséquences négatives sur des droits fondamentaux garantis par la Charte. En particulier, si le système d'IA n'est pas entraîné avec des données de haute qualité, ne répond pas aux exigences voulues en termes de performance, d'exactitude ou de robustesse, ou n'est pas correctement conçu et testé avant d'être mis sur le marché ou mis en service, il risque de traiter des personnes de manière discriminatoire ou, plus généralement, incorrecte ou injuste. En outre, l'exercice de droits fondamentaux procéduraux importants, tels que le droit à un recours effectif et à accéder à un tribunal impartial, ainsi que les droits de la défense et la présomption d'innocence, pourrait être entravé, en particulier lorsque ces systèmes d'IA ne sont pas suffisamment transparents, explicables et documentés. Il convient donc de classer comme étant à haut risque, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, un certain nombre de systèmes d'IA destinés à être utilisés dans un contexte répressif où l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter des conséquences négatives, conserver la confiance du public et garantir que des comptes soient rendus et que des recours puissent être exercés.

Compte tenu de la nature des activités et des risques y afférents, ces systèmes d'IA à haut risque devraient inclure en particulier les systèmes d'IA destinés à être utilisés par les autorités répressives ou pour leur compte ou par les institutions, organes et organismes de l'Union pour aider les autorités répressives à évaluer le risque qu'une personne physique ne devienne victime d'infractions pénales, tels que les polygraphes et instruments similaires, à évaluer la fiabilité des preuves dans le cadre d'enquêtes ou de poursuites relatives à des infractions pénales, et, dans la mesure où cela n'est pas interdit par le présent règlement, à évaluer le risque d'infraction ou de récidive d'une personne physique non seulement sur la base du profilage de personnes physiques, mais aussi sur la base de l'évaluation des traits de personnalité, des caractéristiques ou des antécédents judiciaires de personnes physiques ou de groupes, à des fins de profilage dans le cadre de la détection d'infractions pénales, d'enquêtes et de poursuites en la matière. Les systèmes d'IA spécifiquement destinés à être utilisés pour des procédures administratives par les autorités fiscales et douanières ainsi que par les cellules de renseignement financier effectuant des tâches administratives d'analyse d'informations dans le cadre de la législation de l'Union relative à la lutte contre le blanchiment des capitaux ne devraient pas être classés comme des systèmes d'IA à haut risque utilisés par les autorités répressives à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. L'utilisation des outils d'IA par les autorités répressives et d'autres autorités pertinentes ne devrait pas devenir un facteur d'inégalité ou d'exclusion. Les conséquences de l'utilisation des outils d'IA sur les droits de la défense des suspects ne devraient pas être ignorées, en particulier la difficulté d'obtenir des informations utiles sur le fonctionnement de ces outils et, partant, la difficulté de saisir la justice pour contester leurs résultats, en particulier pour les personnes physiques faisant l'objet d'une enquête.

- (60) Les systèmes d'IA utilisés dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières touchent des personnes qui se trouvent souvent dans une situation particulièrement vulnérable et qui sont tributaires du résultat des actions des autorités publiques compétentes. L'exactitude, la nature non discriminatoire et la transparence des systèmes d'IA utilisés dans ces contextes sont donc particulièrement importantes pour garantir le respect des droits fondamentaux des personnes concernées, en particulier leurs droits à la libre circulation, à la non-discrimination, à la protection de la vie privée et des données à caractère personnel, à une protection internationale et à une bonne administration. Il convient donc de classer comme étant à haut risque, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou pour leur compte ou par les institutions, organes et organismes de l'Union chargés de tâches dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières, tels que les polygraphes et instruments similaires, pour évaluer certains risques présentés par des personnes physiques entrant sur le territoire d'un État membre ou demandant un visa ou l'asile, et pour aider les autorités publiques compétentes à procéder à l'examen, y compris l'évaluation connexe de la fiabilité des éléments de preuve, des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, aux fins de détecter, de reconnaître ou d'identifier des personnes physiques dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, à l'exception de la vérification des documents de voyage.

Les systèmes d'IA utilisés dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières couverts par le présent règlement devraient être conformes aux exigences procédurales pertinentes fixées par le règlement (CE) n° 810/2009 du Parlement européen et du Conseil³², la directive 2013/32/UE du Parlement européen et du Conseil³³ et tout autre acte législatif pertinent de l'Union. Les systèmes d'IA ne devraient en aucun cas être utilisés par les États membres ou les institutions, organes ou organismes de l'Union dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières comme moyen de contourner les obligations internationales qui leur incombent en vertu de la convention des Nations unies relative au statut des réfugiés, signée à Genève le 28 juillet 1951, telle que modifiée par le protocole du 31 janvier 1967. Ils ne devraient pas non plus être utilisés pour enfreindre de quelque manière que ce soit le principe de non-refoulement ou pour refuser des voies d'accès légales sûres et effectives au territoire de l'Union, y compris le droit à la protection internationale.

-
- ³² Règlement (CE) n° 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).
- ³³ Directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (JO L 180 du 29.6.2013, p. 60).

- (61) Certains systèmes d'IA destinés à être utilisés pour l'administration de la justice et les processus démocratiques devraient être classés comme étant à haut risque, compte tenu de leur incidence potentiellement significative sur la démocratie, l'état de droit, les libertés individuelles ainsi que le droit à un recours effectif et à accéder à un tribunal impartial. En particulier, pour faire face aux risques de biais, d'erreurs et d'opacité, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés par une autorité judiciaire ou pour le compte de celle-ci pour aider les autorités judiciaires à rechercher et à interpréter les faits et la loi, et à appliquer la loi à un ensemble concret de faits. Les systèmes d'IA destinés à être utilisés par des organismes de règlement extrajudiciaire des litiges à ces fins devraient également être considérés comme étant à haut risque lorsque les résultats des procédures de règlement extrajudiciaire des litiges produisent des effets juridiques pour les parties. L'utilisation d'outils d'IA peut soutenir le pouvoir de décision des juges ou l'indépendance judiciaire, mais ne devrait pas les remplacer, car la décision finale doit rester une activité humaine. La classification des systèmes d'IA comme étant à haut risque ne devrait cependant pas s'étendre aux systèmes d'IA destinés à être utilisés pour des activités administratives purement accessoires qui n'ont aucune incidence sur l'administration réelle de la justice dans des cas individuels, telles que l'anonymisation ou la pseudonymisation de décisions judiciaires, de documents ou de données, la communication entre membres du personnel ou les tâches administratives.

- (62) Sans préjudice des règles prévues dans le règlement (UE) 2024/... du Parlement européen et du Conseil³⁴⁺, et afin de faire face aux risques d'ingérence extérieure induite dans le droit de vote consacré à l'article 39 de la Charte et d'effets négatifs sur la démocratie et l'état de droit, les systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums devraient être classés comme étant à haut risque, à l'exception des systèmes d'IA dont les sorties ne touchent pas directement les personnes physiques, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques d'un point de vue administratif et logistique.
- (63) Le fait qu'un système d'IA soit classé comme étant à haut risque au titre du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système est licite au titre d'autres actes législatifs de l'Union ou au titre du droit national compatible avec le droit de l'Union, concernant notamment la protection des données à caractère personnel ou l'utilisation de polygraphes et d'instruments similaires ou d'autres systèmes d'analyse de l'état émotionnel des personnes physiques. Toute utilisation de ce type devrait continuer à être subordonnée aux exigences applicables découlant de la Charte et des actes applicables du droit dérivé de l'Union et du droit national. Le présent règlement ne saurait être considéré comme constituant un fondement juridique pour le traitement des données à caractère personnel, y compris des catégories particulières de données à caractère personnel, le cas échéant, sauf disposition contraire expresse du présent règlement.

³⁴ Règlement (UE) 2024/... du Parlement européen et du Conseil du... relatif à la transparence et au ciblage de la publicité à caractère politique (JO L, ..., ELI: ...).

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement figurant dans le document PE-CONS 90/23 (2021/0381 (COD)) et compléter la note de bas de page correspondante.

(64) Afin d'atténuer les risques liés aux systèmes d'IA à haut risque mis sur le marché ou mis en service et de garantir un niveau élevé de fiabilité, certaines exigences obligatoires devraient s'appliquer aux systèmes d'IA à haut risque, en tenant compte de la destination du système d'IA et du contexte de son utilisation et en fonction du système de gestion des risques à mettre en place par le fournisseur. Les mesures adoptées par les fournisseurs pour se conformer aux exigences obligatoires du présent règlement devraient tenir compte de l'état de la technique généralement reconnu en matière d'IA, et être proportionnées et effectives pour atteindre les objectifs du présent règlement. Reposant sur le nouveau cadre législatif, tel que précisé dans la communication de la Commission intitulée ""Guide bleu" relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022", la règle générale est que plus d'un acte juridique de la législation d'harmonisation de l'Union peuvent être applicables à un produit donné, étant donné que la mise à disposition ou la mise en service ne peut avoir lieu que si le produit est conforme à l'ensemble de la législation d'harmonisation de l'Union applicable. Les dangers des systèmes d'IA couverts par les exigences du présent règlement concernent des aspects différents de ceux qui sont énoncés dans la législation d'harmonisation existante de l'Union, et, par conséquent, les exigences du présent règlement complèteraient l'ensemble existant de la législation d'harmonisation de l'Union. Par exemple, les machines ou les dispositifs médicaux incorporant un système d'IA peuvent présenter des risques qui ne sont pas couverts par les exigences essentielles en matière de santé et de sécurité énoncées dans la législation harmonisée pertinente de l'Union, étant donné que cette législation sectorielle ne traite pas des risques spécifiques aux systèmes d'IA.

Cela implique d'appliquer conjointement et de manière complémentaire les divers actes législatifs. Dans un souci de cohérence, et afin d'éviter une charge administrative et des coûts inutiles, les fournisseurs d'un produit contenant un ou plusieurs systèmes d'IA à haut risque, auxquels s'appliquent les exigences du présent règlement ainsi que les exigences de la législation d'harmonisation de l'Union reposant sur le nouveau cadre législatif et dont la liste figure dans une annexe du présent règlement, devraient disposer d'une certaine souplesse en ce qui concerne les décisions opérationnelles à prendre quant à la manière de garantir de façon optimale qu'un produit contenant un ou plusieurs systèmes d'IA est conforme à l'ensemble des exigences applicables de cette législation harmonisée de l'Union. Cette souplesse pourrait signifier, par exemple, que le fournisseur décide d'intégrer une partie des processus d'essai et de déclaration nécessaires, ainsi que des informations et de la documentation requises en vertu du présent règlement dans la documentation et les procédures existantes requises en vertu de la législation d'harmonisation de l'Union en vigueur reposant sur le nouveau cadre législatif et dont la liste figure en annexe du présent règlement. Cela ne devrait en aucun cas porter atteinte à l'obligation qu'a le fournisseur de se conformer à toutes les exigences applicables.

- (65) Le système de gestion des risques devrait consister en un processus itératif continu planifié et se dérouler sur l'ensemble du cycle de vie d'un système d'IA à haut risque. Ce processus devrait viser à identifier et à atténuer les risques des systèmes d'IA qui se posent pour la santé, la sécurité et les droits fondamentaux. Le système de gestion des risques devrait être régulièrement réexaminé et mis à jour afin de garantir le maintien de son efficacité, ainsi que la justification et la documentation de toutes les décisions et mesures importantes prises en vertu du présent règlement. Ce processus devrait garantir que le fournisseur détermine les risques ou les incidences négatives et mette en œuvre des mesures d'atténuation des risques connus et raisonnablement prévisibles des systèmes d'IA pour la santé, la sécurité et les droits fondamentaux à la lumière de leur destination et de leur mauvaise utilisation raisonnablement prévisible, y compris les risques éventuels découlant de l'interaction entre les systèmes d'IA et l'environnement dans lequel ils fonctionnent. Le système de gestion des risques devrait adopter les mesures de gestion des risques les plus appropriées à la lumière de l'état de la technique en matière d'IA. Lorsqu'il détermine les mesures de gestion des risques les plus appropriées, le fournisseur devrait documenter et expliquer les choix effectués et, le cas échéant, associer des experts et des parties prenantes externes. Lorsqu'il s'agit de déterminer la mauvaise utilisation raisonnablement prévisible des systèmes d'IA à haut risque, le fournisseur devrait couvrir les utilisations des systèmes d'IA dont on peut raisonnablement prévoir, bien qu'elles ne soient pas directement couvertes par la destination et prévues dans la notice d'utilisation, qu'elles résultent d'un comportement humain aisément prévisible dans le contexte des caractéristiques et de l'utilisation spécifiques d'un système d'IA donné. Toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé, la sécurité ou les droits fondamentaux, devraient figurer dans la notice d'utilisation fournie par le fournisseur. Il s'agit de veiller à ce que le déploieur en ait connaissance et en tienne compte lors de l'utilisation du système d'IA à haut risque. La détermination et la mise en œuvre de mesures d'atténuation des risques en cas de mauvaise utilisation prévisible au titre du présent règlement ne devraient pas nécessiter de la part du fournisseur, pour remédier à la mauvaise utilisation prévisible, des mesures d'entraînement supplémentaires spécifiques pour le système d'IA à haut risque. Les fournisseurs sont toutefois encouragés à envisager de telles mesures d'entraînement supplémentaires pour atténuer les mauvaises utilisations raisonnablement prévisibles, si cela est nécessaire et approprié.

- (66) Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la gestion des risques, la qualité et la pertinence des jeux de données utilisés, la documentation technique et la tenue de registres, la transparence et la fourniture d'informations aux déployeurs, le contrôle humain, ainsi que la robustesse, l'exactitude et la sécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux. Aucune autre mesure moins contraignante pour le commerce n'étant raisonnablement disponible, ces exigences ne constituent pas des restrictions injustifiées aux échanges.

(67) Les données de haute qualité et l'accès à ces données jouent un rôle essentiel pour ce qui est de fournir une structure et d'assurer le bon fonctionnement de nombreux systèmes d'IA, en particulier lorsque des techniques axées sur l'entraînement de modèles sont utilisées, afin de garantir que le système d'IA à haut risque fonctionne comme prévu et en toute sécurité et qu'il ne devient pas une source de discrimination interdite par le droit de l'Union. Les jeux de données d'entraînement, de validation et de test de haute qualité nécessitent la mise en œuvre de pratiques de gouvernance et de gestion des données appropriées. Les jeux de données d'entraînement, de validation et de test, y compris les étiquettes, devraient être pertinents, suffisamment représentatifs et, dans toute la mesure du possible, exempts d'erreurs et complets au regard de la destination du système. Afin de faciliter le respect du droit de l'Union sur la protection des données, tel que le règlement (UE) 2016/679, les pratiques en matière de gouvernance et de gestion des données devraient inclure, dans le cas des données à caractère personnel, la transparence quant à la finalité initiale de la collecte des données. Les jeux de données devraient également posséder les propriétés statistiques voulues, y compris en ce qui concerne les personnes ou groupes de personnes pour lesquels le système d'IA à haut risque est destiné à être utilisé, en accordant une attention particulière à l'atténuation des éventuels biais dans les jeux de données qui sont susceptibles de porter atteinte à la santé et à la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de se traduire par une discrimination interdite par le droit de l'Union, en particulier lorsque les données de sortie influencent les entrées pour les opérations futures ("boucles de rétroaction"). Des biais peuvent, par exemple, être inhérents à des jeux de données sous-jacents, en particulier lorsque des données historiques sont utilisées, ou générés lorsque les systèmes sont mis en œuvre dans des conditions réelles.

Les résultats produits par les systèmes d'IA pourraient être influencés par ces biais inhérents, qui ont tendance à se renforcer progressivement et ainsi à perpétuer et à amplifier les discriminations existantes, en particulier pour les personnes appartenant à certains groupes vulnérables, y compris les groupes ethniques ou raciaux. L'exigence selon laquelle les jeux de données doivent être dans toute la mesure du possible complets et exempts d'erreurs ne devrait pas avoir d'effet sur l'utilisation de techniques respectueuses de la vie privée dans le contexte du développement et de la mise à l'essai des systèmes d'IA. En particulier, les jeux de données devraient prendre en considération, dans la mesure requise au regard de leur destination, les propriétés, les caractéristiques ou les éléments qui sont propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA est destiné à être utilisé. Les exigences relatives à la gouvernance des données peuvent être respectées en faisant appel à des tiers qui proposent des services de conformité certifiés, y compris la vérification de la gouvernance des données, l'intégrité des jeux de données et les pratiques d'entraînement, de validation et de mise à l'essai des données, dans la mesure où le respect des exigences du présent règlement en matière de données est garanti.

- (68) Pour le développement et l'évaluation de systèmes d'IA à haut risque, certains acteurs, tels que les fournisseurs, les organismes notifiés et d'autres entités concernées, telles que les pôles européens d'innovation numérique, les installations d'expérimentation et d'essai et les centres de recherche, devraient être en mesure d'avoir accès à des jeux de données de haute qualité dans leurs domaines d'activité liés au présent règlement et d'utiliser de tels jeux de données. Les espaces européens communs des données créés par la Commission et la facilitation du partage de données d'intérêt public entre les entreprises et avec le gouvernement seront essentiels pour fournir un accès fiable, responsable et non discriminatoire à des données de haute qualité pour l'entraînement, la validation et la mise à l'essai des systèmes d'IA. Par exemple, dans le domaine de la santé, l'espace européen des données de santé facilitera l'accès non discriminatoire aux données de santé et l'entraînement d'algorithmes d'IA à l'aide de ces jeux de données, d'une manière respectueuse de la vie privée, sûre, rapide, transparente et digne de confiance, et avec une gouvernance institutionnelle appropriée. Les autorités compétentes concernées, y compris les autorités sectorielles, qui fournissent ou facilitent l'accès aux données peuvent aussi faciliter la fourniture de données de haute qualité pour l'entraînement, la validation et la mise à l'essai des systèmes d'IA.
- (69) Le droit au respect de la vie privée et à la protection des données à caractère personnel doit être garanti tout au long du cycle de vie du système d'IA. À cet égard, les principes de minimisation et de protection des données dès la conception et par défaut, tels qu'énoncés dans le droit de l'Union sur la protection des données, sont applicables lorsque des données à caractère personnel sont traitées. Les mesures prises par les fournisseurs pour garantir le respect de ces principes peuvent inclure non seulement l'anonymisation et le cryptage, mais aussi l'utilisation d'une technologie qui permet l'introduction d'algorithmes dans les données ainsi que l'entraînement des systèmes d'IA sans transmission entre parties ou copie des données brutes ou structurées elles-mêmes, sans préjudice des exigences en matière de gouvernance des données prévues par le présent règlement.

- (70) Afin de protéger le droit d'autrui contre la discrimination qui pourrait résulter des biais dans les systèmes d'IA, les fournisseurs devraient, à titre exceptionnel, et dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques et à la suite de l'application de toutes les conditions applicables prévues par le présent règlement en plus des conditions énoncées dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680, être en mesure de traiter également des catégories particulières de données à caractère personnel, pour des raisons d'intérêt public important au sens de l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et de l'article 10, paragraphe 2, point g), du règlement (UE) 2018/1725.
- (71) Il est essentiel de disposer d'informations compréhensibles sur la manière dont les systèmes d'IA à haut risque ont été développés et sur leur fonctionnement tout au long de leur durée de vie afin de permettre la traçabilité de ces systèmes, de vérifier le respect des exigences du présent règlement et de surveiller le fonctionnement des systèmes en question et d'assurer leur surveillance après commercialisation. Cela nécessite la tenue de registres et la disponibilité d'une documentation technique contenant les informations nécessaires pour évaluer la conformité du système d'IA avec les exigences pertinentes et faciliter la surveillance après commercialisation. Ces informations devraient notamment porter sur les caractéristiques générales, les capacités et les limites du système, sur les algorithmes, les données et les processus d'entraînement, de mise à l'essai et de validation utilisés, ainsi que sur le système de gestion des risques mis en place et être établies de façon claire et exhaustive. La documentation technique devrait être dûment tenue à jour tout au long de la durée de vie du système d'IA. Par ailleurs, les systèmes d'IA à haut risque devraient permettre, sur le plan technique, l'enregistrement automatique des événements, au moyen de journaux, tout au long de la durée de vie du système.

(72) Afin de répondre aux préoccupations liées à l'opacité et à la complexité de certains systèmes d'IA et d'aider les déployeurs à remplir les obligations qui leur incombent en vertu du présent règlement, la transparence devrait être requise pour les systèmes d'IA à haut risque avant leur mise sur le marché ou leur mise en service. Les systèmes d'IA à haut risque devraient être conçus de manière à permettre aux déployeurs de comprendre le fonctionnement du système d'IA, d'évaluer sa fonctionnalité et de comprendre ses forces et ses limites. Les systèmes d'IA à haut risque devraient être accompagnés d'informations appropriées sous la forme d'une notice d'utilisation. Ces informations devraient inclure les caractéristiques, les capacités et les limites de la performance du système d'IA. Il s'agirait des informations sur les éventuelles circonstances connues et prévisibles liées à l'utilisation du système d'IA à haut risque, y compris l'action des déployeurs susceptible d'influencer le comportement et la performance du système, dans le cadre desquelles le système d'IA peut entraîner des risques pour la santé, la sécurité et les droits fondamentaux, sur les changements qui ont été déterminés au préalable et évalués à des fins de conformité par le fournisseur et sur les mesures de contrôle humain pertinentes, y compris les mesures visant à faciliter l'interprétation des sorties du système d'IA par les déployeurs. La transparence, y compris la notice d'utilisation jointe au système, devrait aider les déployeurs à utiliser celui-ci et à prendre des décisions en connaissance de cause. Les déployeurs devraient, entre autres, être mieux à même de faire le bon choix quant au système qu'ils ont l'intention d'utiliser à la lumière des obligations qui leur sont applicables, d'être informés sur les utilisations prévues et interdites et d'utiliser le système d'IA correctement et le cas échéant. Afin d'améliorer la lisibilité et l'accessibilité des informations figurant dans la notice d'utilisation, il convient, le cas échéant, d'inclure des exemples illustratifs, par exemple sur les limitations et sur les utilisations prévues et interdites du système d'IA. Les fournisseurs devraient veiller à ce que toute la documentation, y compris la notice d'utilisation, contienne des informations utiles, complètes, accessibles et compréhensibles, compte tenu des besoins et des connaissances prévisibles des déployeurs visés. La notice d'utilisation devrait être mise à disposition dans une langue aisément compréhensible par les déployeurs visés, déterminée par l'État membre concerné.

- (73) Les systèmes d'IA à haut risque devraient être conçus et développés de manière à ce que les personnes physiques puissent superviser leur fonctionnement et veiller à ce qu'ils soient utilisés comme prévu et à ce que leurs incidences soient prises en compte tout au long de leur cycle de vie. À cette fin, des mesures appropriées de contrôle humain devraient être établies par le fournisseur du système avant sa mise sur le marché ou sa mise en service. En particulier, le cas échéant, de telles mesures devraient garantir que le système est soumis à des contraintes opérationnelles intégrées qui ne peuvent pas être ignorées par le système lui-même, que le système répond aux ordres de l'opérateur humain et que les personnes physiques auxquelles le contrôle humain a été confié ont les compétences, la formation et l'autorité nécessaires pour s'acquitter de ce rôle. Il est également essentiel, le cas échéant, de veiller à ce que les systèmes d'IA à haut risque comprennent des mécanismes destinés à guider et à informer une personne physique à laquelle le contrôle humain a été confié, afin qu'elle puisse décider en connaissance de cause s'il faut intervenir, à quel moment et de quelle manière, pour éviter des conséquences négatives ou des risques, ou arrêter le système s'il ne fonctionne pas comme prévu. Compte tenu des conséquences importantes pour les personnes en cas d'erreur dans les correspondances établies par certains systèmes d'identification biométrique, il convient de prévoir pour ces systèmes une exigence de contrôle humain accru, de manière à ce qu'aucune mesure ou décision ne puisse être prise par le déployeur sur la base de l'identification obtenue par le système, à moins qu'elle n'ait été vérifiée et confirmée séparément par au moins deux personnes physiques. Ces personnes pourraient provenir d'une ou de plusieurs entités et compter parmi elles la personne qui fait fonctionner le système ou l'utilise. Cette exigence ne devrait pas entraîner de charges ou de retards inutiles, et il pourrait suffire que les vérifications effectuées séparément par les différentes personnes soient automatiquement enregistrées dans les journaux générés par le système. Compte tenu des spécificités des domaines que sont les activités répressives, la migration, les contrôles aux frontières et l'asile, cette exigence ne devrait pas s'appliquer lorsque le droit de l'Union ou le droit national considère que cette application est disproportionnée.

(74) Les systèmes d'IA à haut risque devraient produire des résultats d'une qualité constante tout au long de leur cycle de vie et assurer un niveau approprié d'exactitude, de robustesse et de cybersécurité, au vu de leur destination et conformément à l'état de la technique généralement reconnu. La Commission et les organisations et parties prenantes concernées sont encouragées à tenir dûment compte de l'atténuation des risques et des incidences négatives du système d'IA. Le niveau attendu des indicateurs de performance devrait être indiqué dans la notice d'utilisation jointe au système. Les fournisseurs sont instamment invités à communiquer ces informations aux déployeurs d'une manière claire et aisément compréhensible, sans malentendus ou déclarations trompeuses. Le droit de l'Union en matière de métrologie légale, y compris les directives 2014/31/UE³⁵ et 2014/32/UE³⁶ du Parlement européen et du Conseil, vise à garantir l'exactitude des mesures et à contribuer à la transparence et à la loyauté des transactions commerciales. Dans ce contexte, en coopération avec les parties prenantes et organisations concernées, telles que les autorités de métrologie et d'étalonnage des performances, la Commission devrait encourager, le cas échéant, l'élaboration de critères de référence et de méthodes de mesure pour les systèmes d'IA. Ce faisant, la Commission devrait prendre note des partenaires internationaux travaillant sur la métrologie et les indicateurs de mesure pertinents relatifs à l'IA et collaborer avec ceux-ci.

³⁵ Directive 2014/31/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des instruments de pesage à fonctionnement non automatique (JO L 96 du 29.3.2014, p. 107).

³⁶ Directive 2014/32/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'instruments de mesure (JO L 96 du 29.3.2014, p. 149).

- (75) La robustesse technique est une exigence essentielle pour les systèmes d'IA à haut risque. Il convient qu'ils soient résilients face aux comportements préjudiciables ou, plus généralement, indésirables pouvant résulter de limites intrinsèques aux systèmes ou dues à l'environnement dans lequel les systèmes fonctionnent (par exemple, les erreurs, les défaillances, les incohérences et les situations inattendues). Par conséquent, des mesures techniques et organisationnelles devraient être prises pour garantir la robustesse des systèmes d'IA à haut risque, par exemple en concevant et développant des solutions techniques appropriées pour prévenir ou réduire au minimum les comportements préjudiciables ou, plus généralement, indésirables. Ces solutions techniques peuvent comprendre, par exemple, des mécanismes permettant au système d'interrompre son fonctionnement en toute sécurité (mesures de sécurité après défaillance) en présence de certaines anomalies ou en cas de fonctionnement en dehors de certaines limites déterminées au préalable. L'absence de protection contre ces risques pourrait avoir des incidences sur la sécurité ou entraîner des violations des droits fondamentaux, par exemple en raison de décisions erronées ou de sorties inexactes ou biaisées générées par le système d'IA.
- (76) La cybersécurité joue un rôle crucial pour ce qui est de garantir la résilience des systèmes d'IA face aux tentatives de détourner leur utilisation, leur comportement ou leur performance ou de compromettre leurs propriétés de sûreté par des tiers malveillants exploitant les vulnérabilités du système. Les cyberattaques contre les systèmes d'IA peuvent passer par des ressources propres à l'IA, telles que les jeux de données d'entraînement (par exemple pour l'empoisonnement de données) ou l'entraînement des modèles (par exemple pour des attaques contradictoires ou des attaques par inférence d'appartenance), ou exploiter les vulnérabilités des ressources numériques du système d'IA ou de l'infrastructure TIC sous-jacente. Pour garantir un niveau de cybersécurité adapté aux risques, des mesures appropriées, telles que des contrôles de sécurité, devraient donc être prises par les fournisseurs de systèmes d'IA à haut risque, en tenant également compte, si nécessaire, de l'infrastructure TIC sous-jacente.

(77) Sans préjudice des exigences relatives à la robustesse et à l'exactitude énoncées dans le présent règlement, les systèmes d'IA à haut risque qui relèvent du champ d'application du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, conformément audit règlement, peuvent démontrer leur conformité avec les exigences de cybersécurité du présent règlement en satisfaisant aux exigences essentielles de cybersécurité énoncées audit règlement. Lorsqu'ils satisfont aux exigences essentielles du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, les systèmes d'IA à haut risque devraient être réputés conformes aux exigences de cybersécurité énoncées dans le présent règlement dans la mesure où le respect de ces exigences est démontré dans la déclaration UE de conformité, ou dans des parties de celle-ci, délivrée en vertu dudit règlement. À cette fin, l'évaluation des risques en matière de cybersécurité associés à un produit comportant des éléments numériques classé comme système d'IA à haut risque conformément au présent règlement, effectuée en vertu du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, devrait tenir compte des risques pesant sur la cyberrésilience d'un système d'IA en ce qui concerne les tentatives de tiers non autorisés de modifier son utilisation, son comportement ou sa performance, y compris les vulnérabilités spécifiques à l'IA telles que l'empoisonnement des données ou les attaques hostiles, ainsi que, le cas échéant, les risques pesant sur les droits fondamentaux, comme l'exige le présent règlement.

(78) La procédure d'évaluation de la conformité prévue par le présent règlement devrait s'appliquer en ce qui concerne les exigences essentielles de cybersécurité d'un produit comportant des éléments numériques relevant du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et classé comme système d'IA à haut risque en vertu du présent règlement. Toutefois, l'application de cette règle ne devrait pas entraîner de réduction du niveau d'assurance nécessaire pour les produits critiques comportant des éléments numériques couverts par le règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques. Par conséquent, par dérogation à cette règle, les systèmes d'IA à haut risque qui relèvent du champ d'application du présent règlement et sont également considérés comme des produits critiques importants comportant des éléments numériques en vertu du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe du présent règlement, sont soumis aux dispositions relatives à l'évaluation de la conformité du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques en ce qui concerne les exigences essentielles de cybersécurité énoncées dans ledit règlement. Dans ce cas, les dispositions respectives relatives à l'évaluation de la conformité fondée sur le contrôle interne énoncées à l'annexe du présent règlement devraient s'appliquer à tous les autres aspects couverts par le présent règlement. En s'appuyant sur les connaissances et l'expertise de l'ENISA en ce qui concerne la politique de cybersécurité et les tâches qui lui sont confiées en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil³⁷, la Commission devrait coopérer avec l'ENISA sur les questions liées à la cybersécurité des systèmes d'IA.

³⁷ Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

- (79) Il convient qu'une personne physique ou morale spécifique, définie comme étant le fournisseur, assume la responsabilité de la mise sur le marché ou de la mise en service d'un système d'IA à haut risque, indépendamment du fait que cette personne physique ou morale soit ou non la personne qui a conçu ou développé le système.
- (80) En leur qualité de signataires de la convention des Nations unies relative aux droits des personnes handicapées, l'Union et les États membres sont légalement tenus de protéger les personnes handicapées contre la discrimination et de promouvoir leur égalité, de veiller à ce que les personnes handicapées aient accès, au même titre que les autres, aux technologies et aux systèmes d'information et de communication, ainsi que de garantir le respect de leur vie privée. Compte tenu de l'importance et de l'utilisation croissantes des systèmes d'IA, l'application des principes de conception universelle à toutes les nouvelles technologies et à tous les nouveaux services devrait garantir un accès complet et égal à toute personne potentiellement concernée par les technologies d'IA ou les utilisant, y compris les personnes handicapées, d'une manière qui tienne pleinement compte de leur dignité et de leur diversité intrinsèques. Il est donc essentiel que les fournisseurs garantissent la pleine conformité avec les exigences en matière d'accessibilité, y compris la directive (UE) 2016/2102 du Parlement européen et du Conseil³⁸ et la directive (UE) 2019/882. Les fournisseurs devraient veiller au respect de ces exigences dès la conception. Les mesures nécessaires devraient donc être aussi intégrées que possible dans la conception des systèmes d'IA à haut risque.

³⁸ Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

- (81) Le fournisseur devrait mettre en place un système solide de gestion de la qualité, garantir le respect de la procédure d'évaluation de la conformité requise, rédiger la documentation pertinente et mettre en place un système solide de surveillance après commercialisation. Les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des obligations en matière de systèmes de gestion de la qualité en vertu du droit sectoriel pertinent de l'Union devraient avoir la possibilité d'intégrer les éléments du système de gestion de la qualité prévus par le présent règlement dans le système de gestion de la qualité existant prévu dans cet autre droit sectoriel de l'Union. La complémentarité entre le présent règlement et le droit sectoriel existant de l'Union devrait également être prise en compte dans les futures activités ou orientations de normalisation de la Commission. Les autorités publiques qui mettent en service des systèmes d'IA à haut risque destinés à être utilisés exclusivement par elles peuvent adopter et mettre en œuvre les règles relatives au système de gestion de la qualité dans le cadre du système de gestion de la qualité adopté au niveau national ou régional, selon le cas, en tenant compte des spécificités du secteur, ainsi que des compétences et de l'organisation de l'autorité publique concernée.

- (82) Pour permettre le contrôle de l'application du présent règlement et créer des conditions de concurrence équitables pour les opérateurs, et compte tenu des différentes formes de mise à disposition des produits numériques, il est important de veiller à ce que, en toutes circonstances, une personne établie dans l'Union puisse fournir aux autorités toutes les informations nécessaires sur la conformité d'un système d'IA. Par conséquent, avant de mettre leurs systèmes d'IA à disposition dans l'Union, les fournisseurs établis dans des pays tiers devraient nommer, par mandat écrit, un mandataire établi dans l'Union. Ce mandataire joue un rôle capital en ce sens qu'il veille à la conformité des systèmes d'IA à haut risque mis sur le marché ou mis en service dans l'Union par des fournisseurs qui ne sont pas établis dans l'Union et sert à ces derniers de point de contact établi dans l'Union.
- (83) Compte tenu de la nature et de la complexité de la chaîne de valeur des systèmes d'IA, et conformément au nouveau cadre législatif, il est essentiel de garantir la sécurité juridique et de faciliter le respect du présent règlement. Par conséquent, il est nécessaire de préciser le rôle et les obligations spécifiques des opérateurs concernés tout au long de ladite chaîne de valeur, tels que les importateurs et les distributeurs qui peuvent contribuer au développement des systèmes d'IA. Dans certaines situations, ces opérateurs pourraient jouer plus d'un rôle en même temps et devraient donc remplir toutes les obligations pertinentes associées à ces rôles. Par exemple, un opérateur pourrait agir à la fois en tant que distributeur et importateur.

- (84) Afin de garantir la sécurité juridique, il est nécessaire de préciser que, dans certaines conditions particulières, tout distributeur, importateur, déployeur ou autre tiers devrait être considéré comme un fournisseur d'un système d'IA à haut risque et, par conséquent, assumer toutes les obligations correspondantes. Tel serait le cas si cette partie met son nom ou sa marque sur un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles stipulant que les obligations sont attribuées d'une autre manière. Tel serait aussi le cas si cette partie apporte une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service et de telle sorte qu'il demeure un système d'IA à haut risque conformément au présent règlement, ou si elle modifie la destination d'un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé comme étant à haut risque et qui a déjà été mis sur le marché ou mis en service, de telle sorte que le système d'IA devient un système d'IA à haut risque conformément au présent règlement. Ces dispositions devraient s'appliquer sans préjudice de dispositions plus spécifiques établies dans certains actes législatifs de l'Union en matière d'harmonisation reposant sur le nouveau cadre législatif avec lesquels le présent règlement devrait s'appliquer. Par exemple, l'article 16, paragraphe 2, du règlement (UE) 2017/745, qui dispose que certaines modifications ne devraient pas être considérées comme des modifications d'un dispositif susceptibles d'influer sur sa conformité avec les exigences applicables, devrait continuer de s'appliquer aux systèmes d'IA à haut risque constituant des dispositifs médicaux au sens dudit règlement.

- (85) Les systèmes d'IA à usage général peuvent être utilisés comme des systèmes d'IA à haut risque en tant que tels ou comme des composants d'autres systèmes d'IA à haut risque. Dès lors, en raison de leur nature particulière, et afin de garantir un partage équitable des responsabilités tout au long de la chaîne de valeur de l'IA, les fournisseurs de systèmes d'IA à usage général, indépendamment du fait que ces systèmes puissent être utilisés comme des systèmes d'IA à haut risque en tant que tels par d'autres fournisseurs ou comme des composants de systèmes d'IA à haut risque, et sauf dispositions contraires du présent règlement, devraient coopérer étroitement avec les fournisseurs des systèmes d'IA à haut risque concernés afin de leur permettre de se conformer aux obligations pertinentes prévues par le présent règlement et avec les autorités compétentes établies en vertu du présent règlement.
- (86) Lorsque, dans les conditions prévues par le présent règlement, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA ne devrait plus être considéré comme le fournisseur aux fins du présent règlement, et lorsque ce fournisseur n'a pas expressément exclu le changement du système d'IA en un système d'IA à haut risque, ce fournisseur devrait néanmoins coopérer étroitement, mettre à disposition les informations nécessaires et fournir l'accès technique raisonnablement attendu et toute autre assistance qui sont requis pour le respect des obligations énoncées dans le présent règlement, notamment en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque.
- (87) En outre, lorsqu'un système d'IA à haut risque qui est un composant de sécurité d'un produit relevant du champ d'application de la législation d'harmonisation de l'Union reposant sur le nouveau cadre législatif n'est pas mis sur le marché ou mis en service indépendamment du produit, le fabricant du produit défini par cette législation devrait se conformer aux obligations du fournisseur établies dans le présent règlement et devrait, en particulier, garantir que le système d'IA intégré dans le produit final est conforme aux exigences du présent règlement.

- (88) Tout au long de la chaîne de valeur de l'IA, plusieurs parties fournissent souvent des systèmes, des outils et des services d'IA, mais aussi des composants ou des processus que le fournisseur intègre dans le système d'IA avec plusieurs objectifs, dont l'entraînement de modèles, le réentraînement de modèles, la mise à l'essai et l'évaluation de modèles, l'intégration dans des logiciels ou d'autres aspects du développement de modèles. Ces parties ont un rôle important à jouer dans la chaîne de valeur vis-à-vis du fournisseur du système d'IA à haut risque dans lequel leurs systèmes, outils, services, composants ou processus d'IA sont intégrés, et devraient fournir à ce fournisseur, en vertu d'un accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaires sur la base de l'état de la technique généralement reconnu, afin de lui permettre de se conformer pleinement aux obligations énoncées dans le présent règlement, sans compromettre leurs propres droits de propriété intellectuelle ou secrets d'affaires.
- (89) Les tiers qui rendent accessibles au public des outils, services, processus ou composants d'IA autres que des modèles d'IA à usage général ne devraient pas être tenus de se conformer aux exigences visant les responsabilités tout au long de la chaîne de valeur de l'IA, en particulier à l'égard du fournisseur qui les a utilisés ou intégrés, lorsque ces outils, services, processus ou composants d'IA sont rendus accessibles sous licence libre et ouverte. Les développeurs d'outils, de services, de processus ou de composants d'IA libres et ouverts autres que les modèles d'IA à usage général devraient être encouragés à mettre en œuvre des pratiques documentaires largement adoptées, telles que les cartes modèles et les fiches de données, afin d'accélérer le partage d'informations tout au long de la chaîne de valeur de l'IA, ce qui permettrait de promouvoir des systèmes d'IA fiables dans l'Union.

- (90) La Commission pourrait élaborer et recommander des clauses contractuelles types volontaires à établir entre les fournisseurs de systèmes d'IA à haut risque et les tiers qui fournissent des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans les systèmes d'IA à haut risque, afin de faciliter la coopération tout au long de la chaîne de valeur. Lorsqu'elle élabore des clauses contractuelles types volontaires, la Commission devrait aussi tenir compte des éventuelles exigences contractuelles applicables dans des secteurs ou des activités spécifiques.
- (91) Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux potentiellement associés à leur utilisation, notamment en ce qui concerne la nécessité d'assurer un suivi adéquat de la performance d'un système d'IA dans un contexte réel, il convient de définir des responsabilités spécifiques pour les déployeurs. Les déployeurs devraient en particulier prendre des mesures techniques et organisationnelles appropriées pour pouvoir utiliser les systèmes d'IA à haut risque conformément à la notice d'utilisation, et certaines autres obligations devraient être prévues en ce qui concerne la surveillance du fonctionnement des systèmes d'IA et la tenue de registres, selon le cas. En outre, les déployeurs devraient veiller à ce que les personnes chargées de mettre en œuvre la notice d'utilisation et au contrôle humain des systèmes énoncées dans le présent règlement possèdent les compétences nécessaires, en particulier un niveau adéquat de maîtrise, de formation et d'autorité en matière d'IA pour s'acquitter correctement de ces tâches. Ces obligations devraient être sans préjudice des autres obligations des déployeurs en ce qui concerne les systèmes d'IA à haut risque en vertu du droit de l'Union ou du droit national.

(92) Le présent règlement est sans préjudice de l'obligation qu'ont les employeurs d'informer ou d'informer et de consulter les travailleurs ou leurs représentants en vertu du droit et des pratiques nationales ou de l'Union, y compris la directive 2002/14/CE du Parlement européen et du Conseil³⁹, sur les décisions de mise en service ou d'utilisation de systèmes d'IA. Il reste nécessaire de veiller à ce que les travailleurs et leurs représentants soient informés du déploiement prévu de systèmes d'IA à haut risque sur le lieu de travail lorsque les conditions de cette obligation d'information ou d'information et de consultation figurant dans d'autres instruments juridiques ne sont pas remplies. En outre, ce droit à l'information est accessoire et nécessaire à l'objectif de protection des droits fondamentaux qui sous-tend le présent règlement. Par conséquent, il convient de prévoir une obligation d'information à cet effet dans le présent règlement, sans porter atteinte aux droits existants des travailleurs.

³⁹ Directive 2002/14/CE du Parlement européen et du Conseil du 11 mars 2002 établissant un cadre général relatif à l'information et la consultation des travailleurs dans la Communauté européenne (JO L 80 du 23.3.2002, p. 29).

- (93) Si des risques liés aux systèmes d'IA peuvent découler de la manière dont ces systèmes sont conçus, ils peuvent également provenir de la manière dont ces systèmes d'IA sont utilisés. Les déployeurs de systèmes d'IA à haut risque jouent donc un rôle essentiel pour ce qui est de garantir la protection des droits fondamentaux, en complétant les obligations du fournisseur lors du développement du système d'IA. Les déployeurs sont les mieux placés pour comprendre comment le système d'IA à haut risque sera utilisé concrètement et peuvent donc identifier les risques importants potentiels qui n'étaient pas prévus au cours de la phase de développement, en raison d'une connaissance plus précise du contexte d'utilisation et des personnes ou groupes de personnes susceptibles d'être concernés, y compris les groupes vulnérables. Les déployeurs de systèmes d'IA à haut risque énumérés dans une annexe du présent règlement contribuent également de façon essentielle à informer les personnes physiques et devraient, lorsqu'ils prennent des décisions ou facilitent la prise de décisions concernant des personnes physiques, selon le cas, informer lesdites personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque. Cette information devrait comprendre la destination du système et le type de décisions prises. Les déployeurs devraient aussi informer les personnes physiques de leur droit à une explication prévu par le présent règlement. En ce qui concerne les systèmes d'IA à haut risque utilisés à des fins répressives, cette obligation devrait être mise en œuvre conformément à l'article 13 de la directive (UE) 2016/680.

- (94) Tout traitement de données biométriques intervenant dans l'utilisation de systèmes d'IA à des fins d'identification biométrique de nature répressive doit être conforme à l'article 10 de la directive (UE) 2016/680, qui n'autorise un tel traitement que lorsque cela est strictement nécessaire, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre. Une telle utilisation, lorsqu'elle est autorisée, doit également respecter les principes énoncés à l'article 4, paragraphe 1, de la directive (UE) 2016/680, notamment la licéité, la loyauté et la transparence, la limitation des finalités, l'exactitude et la limitation de la conservation.
- (95) Sans préjudice du droit de l'Union applicable, en particulier le règlement (UE) 2016/679 et la directive (UE) 2016/680, et compte tenu de la nature intrusive des systèmes d'identification biométrique à distance a posteriori, l'utilisation de systèmes d'identification biométrique à distance a posteriori devrait être soumise à des garanties. Les systèmes d'identification biométrique à distance a posteriori devraient toujours être utilisés d'une manière proportionnée, légitime et strictement nécessaire, et donc ciblée, en ce qui concerne les personnes à identifier, le lieu et la portée temporelle et fondée sur un jeu de données fermé d'images vidéo légalement acquises. En tout état de cause, les systèmes d'identification biométrique à distance a posteriori ne devraient pas être utilisés dans le cadre d'activités répressives pour mener à une surveillance aveugle. Les conditions d'identification biométrique à distance a posteriori ne devraient en aucun cas constituer une base permettant de contourner les conditions applicables en ce qui concerne l'interdiction et les exceptions strictes pour l'identification biométrique à distance en temps réel.

- (96) Afin de garantir efficacement la protection des droits fondamentaux, les déployeurs de systèmes d'IA à haut risque qui sont des organismes de droit public ou des entités privées fournissant des services publics et des déployeurs de certains systèmes d'IA à haut risque énumérés dans une annexe du présent règlement, tels que des entités bancaires ou d'assurance, devraient procéder à une analyse d'impact de ces systèmes concernant les droits fondamentaux avant de les mettre en service. Les services à caractère public importants pour les personnes peuvent également être fournis par des entités privées. Les entités privées fournissant de tels services publics sont liées à des missions d'intérêt public dans des domaines tels que l'éducation, les soins de santé, les services sociaux, le logement et l'administration de la justice. L'analyse d'impact concernant les droits fondamentaux vise à ce que le déployeur identifie les risques spécifiques pour les droits des personnes ou groupes de personnes susceptibles d'être concernés et à ce qu'il détermine les mesures à prendre en cas de matérialisation de ces risques. L'analyse d'impact devrait être réalisée avant le premier déploiement du système d'IA à haut risque et être mise à jour lorsque le déployeur estime que l'un des facteurs pertinents a changé. L'analyse d'impact devrait identifier les processus pertinents du déployeur dans lesquels le système d'IA à haut risque sera utilisé conformément à sa destination, et devrait indiquer la durée pendant laquelle le système est destiné à être utilisé et selon quelle fréquence ainsi que les catégories spécifiques de personnes physiques et de groupes susceptibles d'être concernés dans le contexte spécifique d'utilisation.

L'analyse devrait aussi déterminer les risques spécifiques de préjudice susceptibles d'avoir une incidence sur les droits fondamentaux de ces personnes ou groupes. Afin que cette analyse soit réalisée correctement, le déployeur devrait tenir compte des informations pertinentes, y compris, mais sans s'y limiter, les informations communiquées par le fournisseur du système d'IA à haut risque dans la notice d'utilisation. À la lumière des risques recensés, les déployeurs devraient déterminer les mesures à prendre en cas de matérialisation de ces risques, y compris, par exemple, les dispositions en matière de gouvernance dans ce contexte spécifique d'utilisation, telles que les dispositions pour le contrôle humain conformément à la notice d'utilisation ou les procédures de traitement des plaintes et de recours, en ce qu'elles pourraient contribuer à atténuer les risques pour les droits fondamentaux dans des cas d'utilisation concrets. Après avoir réalisé cette analyse d'impact, le déployeur devrait en informer l'autorité de surveillance du marché concernée. Le cas échéant, pour recueillir les informations pertinentes nécessaires à la réalisation de l'analyse d'impact, les déployeurs de systèmes d'IA à haut risque, en particulier lorsque des systèmes d'IA sont utilisés dans le secteur public, pourraient associer les parties prenantes concernées, y compris les représentants de groupes de personnes susceptibles d'être concernés par le système d'IA, les experts indépendants et les organisations de la société civile, à la réalisation de cette analyse d'impact et à la conception des mesures à prendre en cas de matérialisation des risques. Le Bureau européen de l'intelligence artificielle (ci-après dénommé "Bureau de l'IA") devrait élaborer un modèle de questionnaire afin de faciliter la mise en conformité et de réduire la charge administrative pesant sur les déployeurs.

(97) La notion de modèles d'IA à usage général devrait être clairement définie et distincte de la notion de systèmes d'IA afin de garantir la sécurité juridique. La définition devrait se fonder sur les principales caractéristiques fonctionnelles d'un modèle d'IA à usage général, en particulier la généralité et la capacité d'exécuter de manière compétente un large éventail de tâches distinctes. Ces modèles sont généralement entraînés avec de grandes quantités de données, au moyen de diverses méthodes, telles que l'apprentissage auto-supervisé, non supervisé ou par renforcement. Les modèles d'IA à usage général peuvent être mis sur le marché de différentes manières, notamment au moyen de bibliothèques, d'interfaces de programmation d'applications (API), de téléchargements directs ou de copies physiques. Ces modèles peuvent être modifiés ou affinés et ainsi se transformer en nouveaux modèles. Bien que les modèles d'IA soient des composants essentiels des systèmes d'IA, ils ne constituent pas en soi des systèmes d'IA. Les modèles d'IA nécessitent l'ajout d'autres composants, tels qu'une interface utilisateur, pour devenir des systèmes d'IA. Les modèles d'IA sont généralement intégrés dans les systèmes d'IA et en font partie. Le présent règlement prévoit des règles spécifiques pour les modèles d'IA à usage général et pour les modèles d'IA à usage général qui présentent des risques systémiques, lesquelles devraient également s'appliquer lorsque ces modèles sont intégrés dans un système d'IA ou en font partie. Il convient de considérer que les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient s'appliquer une fois que ces modèles sont mis sur le marché.

Lorsque le fournisseur d'un modèle d'IA à usage général intègre un propre modèle dans son propre système d'IA qui est mis à disposition sur le marché ou mis en service, ce modèle devrait être considéré comme étant mis sur le marché et, par conséquent, les obligations prévues par le présent règlement pour les modèles devraient continuer de s'appliquer en plus de celles applicables aux systèmes d'IA. Les obligations prévues pour les modèles ne devraient en aucun cas s'appliquer lorsqu'un propre modèle est utilisé pour des processus purement internes qui ne sont pas essentiels à la fourniture d'un produit ou d'un service à des tiers et que les droits des personnes physiques ne sont pas affectés. Compte tenu de leurs effets potentiellement très négatifs, les modèles d'IA à usage général présentant un risque systémique devraient toujours être soumis aux obligations pertinentes prévues par le présent règlement. La définition ne devrait pas couvrir les modèles d'IA utilisés avant leur mise sur le marché aux seules fins d'activités de recherche, de développement et de prototypage. Cela est sans préjudice de l'obligation de se conformer au présent règlement lorsque, à la suite de telles activités, un modèle est mis sur le marché.

- (98) Alors que la généralité d'un modèle pourrait, entre autres, également être déterminée par un nombre de paramètres, les modèles comptant au moins un milliard de paramètres et entraînés à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle devraient être considérés comme présentant une généralité significative et exécutant de manière compétente un large éventail de tâches distinctes.
- (99) Les grands modèles d'IA génératifs sont un exemple typique d'un modèle d'IA à usage général, étant donné qu'ils permettent la production flexible de contenus, tels que du texte, de l'audio, des images ou de la vidéo, qui peuvent aisément s'adapter à un large éventail de tâches distinctes.

- (100) Lorsqu'un modèle d'IA à usage général est intégré dans un système d'IA ou en fait partie, ce système devrait être considéré comme un système d'IA à usage général lorsque, en raison de cette intégration, ce système a la capacité de répondre à divers usages. Un système d'IA à usage général peut être utilisé directement ou être intégré dans d'autres systèmes d'IA.
- (101) Les fournisseurs de modèles d'IA à usage général ont un rôle et une responsabilité particuliers tout au long de la chaîne de valeur de l'IA, étant donné que les modèles qu'ils fournissent peuvent constituer la base d'une série de systèmes en aval, souvent fournis par des fournisseurs en aval, qui nécessitent une bonne compréhension des modèles et de leurs capacités, à la fois pour permettre l'intégration de ces modèles dans leurs produits et pour remplir les obligations qui leur incombent en vertu du présent règlement ou d'autres règlements. Par conséquent, des mesures de transparence proportionnées devraient être prévues, y compris l'élaboration et la tenue à jour de la documentation, et la fourniture d'informations sur le modèle d'IA à usage général en vue de son utilisation par les fournisseurs en aval. La documentation technique devrait être élaborée et tenue à jour par le fournisseur de modèles d'IA à usage général afin qu'elle puisse être mise, sur demande, à la disposition du Bureau de l'IA et des autorités nationales compétentes. L'ensemble minimal d'éléments à inclure dans cette documentation devrait figurer dans des annexes spécifiques du présent règlement. La Commission devrait être habilitée à modifier ces annexes par voie d'actes délégués à la lumière des évolutions technologiques.

- (102) Les logiciels et les données, y compris les modèles, publiés dans le cadre d'une licence libre et ouverte grâce à laquelle ils peuvent être partagés librement et qui permet aux utilisateurs de librement consulter, utiliser, modifier et redistribuer ces logiciels et données ou leurs versions modifiées peuvent contribuer à la recherche et à l'innovation sur le marché et offrir d'importantes possibilités de croissance pour l'économie de l'Union. Les modèles d'IA à usage général publiés sous licence libre et ouverte devraient être considérés comme garantissant des niveaux élevés de transparence et d'ouverture si leurs paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. La licence devrait également être considérée comme libre et ouverte lorsqu'elle permet aux utilisateurs d'exploiter, de copier, de distribuer, d'étudier, de modifier et d'améliorer les logiciels et les données, y compris les modèles, à condition que le fournisseur initial du modèle soit crédité et que les conditions de distribution identiques ou comparables soient respectées.
- (103) Les composants d'IA libres et ouverts couvrent les logiciels et les données, y compris les modèles et les modèles à usage général, outils, services ou processus d'un système d'IA. Les composants d'IA libres et ouverts peuvent être fournis par différents canaux, y compris leur développement dans des référentiels ouverts. Aux fins du présent règlement, les composants d'IA qui sont fournis contre paiement ou monétisés, y compris par la fourniture d'un soutien technique ou d'autres services, notamment au moyen d'une plateforme logicielle, liés au composant d'IA, ou l'utilisation de données à caractère personnel pour des raisons autres qu'aux fins exclusives de l'amélioration de la sécurité, de la compatibilité ou de l'interopérabilité des logiciels, à l'exception des transactions entre micro-entreprises, ne devraient pas bénéficier des exceptions prévues pour les composants d'IA libres et ouverts. La mise à disposition de composants d'IA au moyen de référentiels ouverts ne devrait pas, en soi, constituer une monétisation.

- (104) Les fournisseurs de modèles d'IA à usage général qui sont publiés sous licence libre et ouverte et dont les paramètres, y compris les poids, les informations sur l'architecture des modèles et les informations sur l'utilisation des modèles, sont rendus publics devraient faire l'objet d'exceptions en ce qui concerne les exigences en matière de transparence imposées pour les modèles d'IA à usage général, à moins que les modèles ne puissent être considérés comme présentant un risque systémique, auquel cas le fait que les modèles soient transparents et accompagnés d'une licence ouverte ne devrait pas être considéré comme une raison suffisante pour exclure le respect des obligations prévues par le présent règlement. En tout état de cause, étant donné que la publication de modèles d'IA à usage général sous licence libre et ouverte ne révèle pas nécessairement des informations importantes sur le jeu de données utilisé pour l'entraînement ou de réglage fin du modèle et sur la manière dont le respect de la législation sur le droit d'auteur a été assuré, l'exception prévue pour les modèles d'IA à usage général en ce qui concerne les exigences en matière de transparence ne devrait pas concerner l'obligation de produire un résumé du contenu utilisé pour l'entraînement des modèles ni l'obligation de mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur, en particulier pour identifier et respecter la réservation de droits au titre de l'article 4, paragraphe 3, de la directive (UE) 2019/790 du Parlement européen et du Conseil⁴⁰.

⁴⁰ Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

- (105) Les modèles d'IA à usage général, en particulier les grands modèles d'IA génératifs, capables de générer du texte, des images et d'autres contenus, présentent des possibilités d'innovation uniques mais aussi des défis pour les artistes, les auteurs et les autres créateurs, et la manière dont leur contenu créatif est créé, distribué, utilisé et consommé. Le développement et l'entraînement de ces modèles requièrent un accès à de grandes quantités de texte, d'images, de vidéos et d'autres données. Les techniques de fouille de textes et de données peuvent être largement utilisées dans ce contexte pour extraire et analyser ces contenus, qui peuvent être protégés par le droit d'auteur et les droits voisins. Toute utilisation d'un contenu protégé par le droit d'auteur nécessite l'autorisation du titulaire de droits concerné, à moins que des exceptions et limitations pertinentes en matière de droit d'auteur ne s'appliquent. La directive (UE) 2019/790 a introduit des exceptions et des limitations autorisant les reproductions et extractions d'œuvres ou d'autres objets protégés aux fins de la fouille de textes et de données, sous certaines conditions. En vertu de ces règles, les titulaires de droits peuvent choisir de réserver leurs droits sur leurs œuvres ou autres objets protégés afin d'empêcher la fouille de textes et de données, à moins que celle-ci ne soit effectuée à des fins de recherche scientifique. Lorsque les droits d'exclusion ont été expressément réservés de manière appropriée, les fournisseurs de modèles d'IA à usage général doivent obtenir une autorisation des titulaires de droits s'ils souhaitent procéder à une fouille de textes et de données sur ces œuvres.

- (106) Les fournisseurs qui mettent des modèles d'IA à usage général sur le marché de l'Union devraient veiller au respect des obligations pertinentes prévues par le présent règlement. À cette fin, les fournisseurs de modèles d'IA à usage général devraient mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur et les droits voisins, en particulier pour identifier et respecter la réservation de droits exprimées par les titulaires de droits conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790. Tout fournisseur qui met un modèle d'IA à usage général sur le marché de l'Union devrait se conformer à cette obligation, quelle que soit la juridiction dans laquelle se déroulent les actes pertinents au titre du droit d'auteur qui sous-tendent l'entraînement de ces modèles d'IA à usage général. Cela est nécessaire pour garantir des conditions de concurrence équitables entre les fournisseurs de modèles d'IA à usage général, lorsqu'aucun fournisseur ne devrait pouvoir obtenir un avantage concurrentiel sur le marché de l'Union en appliquant des normes en matière de droit d'auteur moins élevées que celles prévues dans l'Union.

- (107) Afin d'accroître la transparence concernant les données utilisées dans le cadre de l'entraînement préalable et de l'entraînement des modèles d'IA à usage général, y compris le texte et les données protégés par la législation sur le droit d'auteur, il convient que les fournisseurs de ces modèles élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner les modèles d'IA à usage général. Tout en tenant dûment compte de la nécessité de protéger les secrets d'affaires et les informations commerciales confidentielles, ce résumé devrait être généralement complet en termes de contenu plutôt que détaillé sur le plan technique afin d'aider les parties ayant des intérêts légitimes, y compris les titulaires de droits d'auteur, à exercer et à faire respecter les droits que leur confère la législation de l'Union, par exemple en énumérant les principaux jeux ou collections de données utilisés pour entraîner le modèle, tels que les archives de données ou bases de données publiques ou privées de grande ampleur, et en fournissant un texte explicatif sur les autres sources de données utilisées. Il convient que le Bureau de l'IA fournisse un modèle de résumé, qui devrait être simple et utile et permettre au fournisseur de fournir le résumé requis sous forme descriptive.
- (108) En ce qui concerne l'obligation imposée aux fournisseurs de modèles d'IA à usage général de mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur et de mettre à la disposition du public un résumé du contenu utilisé pour l'entraînement, le Bureau de l'IA devrait vérifier si le fournisseur a rempli cette obligation sans vérifier ou évaluer œuvre par œuvre les données d'entraînement en ce qui concerne le respect du droit d'auteur. Le présent règlement n'affecte pas l'application des règles en matière de droit d'auteur prévues par la législation de l'Union.

- (109) Le respect des obligations applicables aux fournisseurs de modèles d'IA à usage général devrait correspondre et être proportionné au type de fournisseur de modèles, excluant la nécessité de se conformer pour les personnes qui développent ou utilisent des modèles à des fins non professionnelles ou de recherche scientifique, lesquelles devraient néanmoins être encouragées à se conformer volontairement à ces exigences. Sans préjudice de la législation de l'Union sur le droit d'auteur, le respect de ces obligations devrait tenir dûment compte de la taille du fournisseur et permettre aux PME, y compris aux jeunes pousses, de recourir à des méthodes simplifiées de mise en conformité qui ne devraient pas représenter un coût excessif et décourager l'utilisation de tels modèles. En cas de modification ou de réglage fin d'un modèle, les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient se limiter à cette modification ou à ce réglage fin, par exemple en complétant la documentation technique existante avec des informations sur les modifications, y compris les nouvelles sources de données d'entraînement, aux fins de conformité avec les obligations relatives à la chaîne de valeur prévues par le présent règlement.

- (110) Les modèles d'IA à usage général pourraient présenter des risques systémiques qui comprennent, sans s'y limiter, tout effet négatif réel ou raisonnablement prévisible en rapport avec des accidents majeurs, des perturbations de secteurs critiques et des conséquences graves pour la santé et la sécurité publiques, tout effet négatif réel ou raisonnablement prévisible sur les processus démocratiques, la sécurité publique et la sécurité économique, et la diffusion de contenus illicites, faux ou discriminatoires. Les risques systémiques devraient être perçus comme augmentant avec les capacités et la portée du modèle, peuvent survenir tout au long du cycle de vie du modèle et sont influencés par les conditions de mauvaise utilisation, la fiabilité du modèle, l'équité et la sécurité du modèle, le niveau d'autonomie du modèle, son accès aux outils, les modalités nouvelles ou combinées, les stratégies de publication et de distribution, le potentiel de suppression des garde-fous et d'autres facteurs. En particulier, les approches internationales ont jusqu'à présent mis en évidence la nécessité de prêter attention aux risques liés à une potentielle mauvaise utilisation intentionnelle ou à des problèmes non intentionnels de contrôle liés à l'alignement sur l'intention humaine, aux risques chimiques, biologiques, radiologiques et nucléaires, tels que les moyens d'abaisser les barrières à l'entrée, y compris pour la mise au point, l'acquisition ou l'utilisation d'armes, aux cybercapacités offensives, tels que les moyens permettant la découverte, l'exploitation ou l'utilisation opérationnelle de vulnérabilités, aux effets de l'interaction et de l'utilisation des outils, y compris, par exemple, la capacité de contrôler les systèmes physiques et d'interférer avec les infrastructures critiques, aux risques liés à la possibilité que les modèles fassent des copies d'eux-mêmes ou "s'auto-reproduisent" ou qu'ils entraînent d'autres modèles, à la manière dont les modèles peuvent donner lieu à des préjugés et des discriminations préjudiciables présentant des risques pour les individus, les communautés ou les sociétés, à la facilitation de la désinformation ou au préjudice porté à la vie privée par des menaces pour les valeurs démocratiques et les droits de l'homme, et au risque qu'un événement particulier entraîne une réaction en chaîne s'accompagnant d'effets négatifs considérables qui pourraient aller jusqu'à affecter toute une ville, tout un secteur d'activité ou toute une communauté.

- (111) Il convient d'établir une méthode de classification des modèles d'IA à usage général en tant que modèle d'IA à usage général présentant des risques systémiques. Étant donné que les risques systémiques résultent de capacités particulièrement élevées, un modèle d'IA à usage général devrait être considéré comme présentant des risques systémiques s'il a des capacités à fort impact, évaluées sur la base de méthodologies et d'outils techniques appropriés, ou une incidence significative sur le marché intérieur en raison de sa portée. Les capacités à fort impact des modèles d'IA à usage général sont des capacités égales ou supérieures aux capacités des modèles d'IA à usage général les plus avancés. L'éventail complet des capacités d'un modèle pourrait être mieux compris après sa mise sur le marché ou lorsque les déployeurs interagissent avec le modèle. Selon l'état de la technique au moment de l'entrée en vigueur du présent règlement, la quantité cumulée de calculs utilisée pour l'entraînement du modèle d'IA à usage général mesurée en opérations en virgule flottante est l'une des approximations pertinentes pour les capacités du modèle. La quantité cumulée de calculs utilisée pour l'entraînement inclut les calculs utilisés pour l'ensemble des activités et méthodes destinées à renforcer les capacités du modèle avant le déploiement, telles que l'entraînement préalable, la production de données synthétiques et le réglage fin. Par conséquent, il convient de fixer un seuil initial d'opérations en virgule flottante, qui, s'il est atteint par un modèle d'IA à usage général, conduit à présumer qu'il s'agit d'un modèle d'IA à usage général présentant des risques systémiques. Ce seuil devrait être ajusté au fil du temps pour tenir compte des évolutions technologiques et industrielles, telles que les améliorations algorithmiques ou l'amélioration de l'efficacité des matériels, et être complété par des critères de référence et des indicateurs pour la capacité du modèle.

À cette fin, le Bureau de l'IA devrait coopérer avec la communauté scientifique, l'industrie, la société civile et d'autres experts. Les seuils, ainsi que les outils et les critères de référence pour l'évaluation des capacités à fort impact, devraient être de bons indicateurs de la généralité et des capacités des modèles d'IA à usage général ainsi que du risque systémique qui y est associé, et pourraient tenir compte de la manière dont le modèle sera mis sur le marché ou du nombre d'utilisateurs qu'il pourrait affecter. Afin de compléter ce système, la Commission devrait avoir la possibilité de prendre des décisions individuelles désignant un modèle d'IA à usage général comme modèle d'IA à usage général présentant un risque systémique s'il est constaté que ce modèle a des capacités ou une incidence équivalentes à celles relevant du seuil fixé. Ces décisions devraient être prises sur la base d'une évaluation globale des critères de désignation des modèles d'IA à usage général présentant un risque systémique énoncés dans une annexe du présent règlement, tels que la qualité ou la taille du jeu de données d'entraînement, le nombre d'utilisateurs professionnels et finaux du modèle, ses modalités d'entrée et de sortie, son niveau d'autonomie et d'évolutivité, ou les outils auxquels il a accès. Sur demande motivée d'un fournisseur dont le modèle a été désigné comme modèle d'IA à usage général présentant un risque systémique, la Commission devrait tenir compte de la demande et peut décider de réévaluer si le modèle d'IA à usage général peut encore être considéré comme présentant un risque systémique.

(112) Il convient également d'établir de façon précise une procédure de classification d'un modèle d'IA à usage général présentant un risque systémique. Il convient de présumer qu'un modèle d'IA à usage général qui atteint le seuil applicable pour les capacités à fort impact est un modèle d'IA à usage général présentant un risque systémique. Le fournisseur devrait informer le Bureau de l'IA au plus tard deux semaines après que les exigences ont été remplies ou qu'il a été établi qu'un modèle d'IA à usage général répondra aux exigences qui conduisent à la présomption. Cela est particulièrement important en ce qui concerne le seuil d'opérations en virgule flottante, car l'entraînement des modèles d'IA à usage général nécessite une planification considérable qui inclut l'allocation préalable des ressources de calcul, et, par conséquent, les fournisseurs de modèles d'IA à usage général sont en mesure de savoir si leur modèle atteindra le seuil avant l'achèvement de l'entraînement. Dans le cadre de cette information, le fournisseur devrait pouvoir démontrer que, en raison de ses caractéristiques spécifiques, un modèle d'IA à usage général ne présente pas, exceptionnellement, de risques systémiques et qu'il ne devrait donc pas être classé comme modèle d'IA à usage général présentant des risques systémiques. Ces éléments d'information sont utiles pour le Bureau de l'IA en ce qu'ils lui permettent d'anticiper la mise sur le marché de modèles d'IA à usage général présentant des risques systémiques, et les fournisseurs peuvent ainsi commencer à coopérer avec le Bureau de l'IA à un stade précoce. Ils sont particulièrement importants en ce qui concerne les modèles d'IA à usage général qu'il est prévu de publier en tant que source ouverte, étant donné que, après la publication des modèles de source ouverte, les mesures nécessaires pour garantir le respect des obligations prévues par le présent règlement peuvent être plus difficiles à mettre en œuvre.

- (113) Si la Commission prend connaissance du fait qu'un modèle d'IA à usage général satisfait aux exigences de classification en tant que modèle d'IA à usage général présentant un risque systémique, qui n'était pas connu auparavant ou dont le fournisseur concerné n'avait pas informé la Commission, celle-ci devrait être habilitée à désigner ce modèle comme tel. Un système d'alertes qualifiées devrait garantir que le Bureau de l'IA est informé par le panel scientifique des modèles d'IA à usage général qui devraient éventuellement être classés comme modèles d'IA à usage général présentant un risque systémique, en plus des activités de suivi du Bureau de l'IA.
- (114) Les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient être soumis non seulement aux obligations prévues pour les fournisseurs de modèles d'IA à usage général mais aussi à des obligations visant à identifier et à atténuer ces risques et à garantir un niveau adéquat de protection de la cybersécurité, que les modèles en question soient fournis en tant que modèles autonomes ou qu'ils soient intégrés dans un système ou un produit d'IA. Pour atteindre ces objectifs, le présent règlement devrait exiger des fournisseurs qu'ils effectuent les évaluations nécessaires des modèles, en particulier avant leur première mise sur le marché, y compris la réalisation et la documentation d'essais contradictoires des modèles, ainsi que, le cas échéant, au moyen d'essais internes ou externes indépendants. En outre, les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient évaluer et atténuer en permanence les risques systémiques, y compris, par exemple, en mettant en place des politiques de gestion des risques, telles que des processus de responsabilité et de gouvernance, en mettant en œuvre une surveillance après commercialisation, en prenant des mesures appropriées tout au long du cycle de vie du modèle et en coopérant avec les acteurs pertinents tout au long de la chaîne de valeur de l'IA.

- (115) Les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient évaluer et atténuer les éventuels risques systémiques. Si, malgré les efforts déployés pour recenser et prévenir les risques liés à un modèle d'IA à usage général susceptible de présenter des risques systémiques, le développement ou l'utilisation du modèle cause un incident grave, le fournisseur de modèle d'IA à usage général devrait, sans retard injustifié, réaliser un suivi de l'incident et communiquer toute information pertinente et toute mesure corrective éventuelle à la Commission et aux autorités nationales compétentes. En outre, les fournisseurs devraient garantir un niveau approprié de protection en matière de cybersécurité en ce qui concerne le modèle et son infrastructure physique, le cas échéant, tout au long du cycle de vie du modèle. La protection en matière de cybersécurité contre les risques systémiques associés à une utilisation malveillante ou à des attaques devrait tenir dûment compte des fuites accidentelles du modèle, des publications non autorisées, du contournement des mesures de sécurité ainsi que de la défense contre les cyberattaques, l'accès non autorisé ou le vol de modèle. Une telle protection pourrait être facilitée par la sécurisation des poids du modèle, des algorithmes, des serveurs et des jeux de données, notamment au moyen de mesures de sécurité opérationnelle relatives à la sécurité de l'information, de politiques spécifiques en matière de cybersécurité, de solutions techniques établies adéquates, et de contrôles de l'accès physique ou informatique, qui soient adaptés aux circonstances particulières et aux risques encourus.

- (116) Le Bureau de l'IA devrait encourager et faciliter l'élaboration, le réexamen et l'adaptation des codes de bonne pratique, en tenant compte des approches internationales. Tous les fournisseurs de modèles d'IA à usage général pourraient être invités à participer. Afin de veiller à ce que les codes de bonne pratique correspondent à l'état de la technique et prennent dûment en compte un ensemble divers de perspectives, le Bureau de l'IA devrait collaborer avec les autorités nationales compétentes concernées et pourrait, selon qu'il convient, consulter les organisations de la société civile et d'autres parties prenantes et experts pertinents, notamment le groupe scientifique, pour l'élaboration de ces codes. Les codes de bonne pratique devraient traiter des obligations incombant aux fournisseurs de modèles d'IA à usage général, et de modèles d'IA à usage général présentant des risques systémiques. En outre, en ce qui concerne les risques systémiques, les codes de bonne pratique devraient contribuer à établir une taxinomie des risques reprenant le type et la nature des risques systémiques au niveau de l'Union, ainsi que leur source. Les codes de bonne pratique devraient également mettre l'accent sur une évaluation des risques et des mesures d'atténuation spécifiques.

- (117) Les codes de bonne pratique devraient constituer un outil central pour assurer le bon respect des obligations qui incombent aux fournisseurs de modèles d'IA à usage général au titre du présent règlement. Les fournisseurs devraient pouvoir s'appuyer sur des codes de bonne pratique pour démontrer qu'ils respectent leurs obligations. Par voie d'actes d'exécution, la Commission pourrait décider d'approuver un code de bonnes pratiques et de lui conférer une validité générale au sein de l'Union ou, à défaut, de fixer des règles communes pour la mise en œuvre des obligations pertinentes si un code de bonnes pratiques ne peut pas être mis au point avant que le présent règlement ne devienne applicable, ou si un tel code n'est pas considéré comme adéquat par le Bureau de l'IA. Dès lors qu'une norme harmonisée est publiée et jugée appropriée par le Bureau de l'IA au regard des obligations pertinentes, les fournisseurs devraient bénéficier de la présomption de conformité lorsqu'ils respectent une norme européenne harmonisée. En outre, les fournisseurs de modèles d'IA à usage général devraient être en mesure de démontrer la conformité en utilisant d'autres moyens adéquats en l'absence de codes de bonne pratique ou de normes harmonisées ou s'ils choisissent de ne pas s'appuyer sur ceux-ci.

(118) Le présent règlement régit les systèmes et modèles d'IA en instituant certaines exigences et obligations visant les acteurs du marché concernés qui les mettent sur le marché, les mettent en service ou les utilisent dans l'Union, complétant ainsi les obligations incombant aux fournisseurs de services intermédiaires qui intègrent de tels systèmes ou modèles dans leurs services relevant du règlement (UE) 2022/2065. Dans la mesure où ces systèmes ou modèles sont intégrés dans des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne, ils sont soumis au cadre de gestion des risques établi par le règlement (UE) 2022/2065. Par conséquent, il devrait être présumé que les obligations correspondantes du présent règlement sont remplies, à moins que des risques systémiques importants non couverts par le règlement (UE) 2022/2065 n'apparaissent et ne soient recensés dans de tels modèles. Dans ce contexte, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont tenus d'évaluer les risques systémiques découlant de la conception, du fonctionnement et de l'utilisation de leurs services, y compris la manière dont la conception des systèmes algorithmiques utilisés dans un service pourrait contribuer à ces risques, ainsi que les risques systémiques découlant de mauvaises utilisations éventuelles. Ces fournisseurs sont également tenus de prendre les mesures d'atténuation appropriées pour assurer le respect des droits fondamentaux.

- (119) Compte tenu du rythme rapide de l'innovation et de l'évolution technologique des services numériques relevant du champ d'application de différents instruments du droit de l'Union, en particulier à la lumière de l'utilisation et de la perception de leurs destinataires, les systèmes d'IA régis par le présent règlement pourraient être fournis en tant que services intermédiaires ou parties de ceux-ci au sens du règlement (UE) 2022/2065, qui devrait être interprété de manière neutre sur le plan technologique. Par exemple, les systèmes d'IA pourraient être utilisés pour fournir des moteurs de recherche en ligne, en particulier, dans la mesure où un système d'IA tel qu'un dialogueur réalise des recherches sur, en principe, tous les sites web, puis en intègre les résultats dans ses connaissances existantes et utilise les connaissances mises à jour pour générer une sortie unique qui combine différentes sources d'information.
- (120) En outre, les obligations imposées aux fournisseurs et aux déployeurs de certains systèmes d'IA au titre du présent règlement afin de permettre la détection et la mention du fait que les sorties produites par ces systèmes sont générées ou manipulées par une IA revêtent une importance particulière pour faciliter la mise en œuvre effective du règlement (UE) 2022/2065. Cela vaut en particulier pour les obligations incombant aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne consistant à recenser et à atténuer les risques systémiques susceptibles de découler de la diffusion de contenus qui ont été générés ou manipulés par une IA, en particulier le risque d'effets négatifs réels ou prévisibles sur les processus démocratiques, le débat public et les processus électoraux, notamment par le biais de la désinformation.

(121) La normalisation devrait jouer un rôle essentiel pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec le présent règlement, suivant les technologies les plus récentes, et de promouvoir l'innovation ainsi que la compétitivité et la croissance dans le marché unique. Le respect des normes harmonisées telles que définies à l'article 2, point 1) c), du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil⁴¹, qui doivent normalement tenir compte des évolutions technologiques les plus récentes, devrait être un moyen pour les fournisseurs de démontrer la conformité avec les exigences du présent règlement. Il convient donc d'encourager une représentation équilibrée des intérêts en associant toutes les parties prenantes concernées à l'élaboration des normes, en particulier les PME, les organisations de consommateurs et les acteurs environnementaux et sociaux, conformément aux articles 5 et 6 du règlement (UE) n° 1025/2012. Afin de faciliter le respect de la législation, les demandes de normalisation devraient être formulées par la Commission sans retard injustifié. Lorsqu'elle élabore les demandes de normalisation, la Commission devrait consulter le forum consultatif et le Comité IA afin de recueillir l'expertise pertinente. Toutefois, en l'absence de références pertinentes à des normes harmonisées, la Commission devrait être en mesure d'établir, au moyen d'actes d'exécution, et après consultation du forum consultatif, des spécifications communes pour certaines exigences au titre du présent règlement.

⁴¹ Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

Les spécifications communes devraient être une solution de repli exceptionnelle pour faciliter l'obligation du fournisseur de se conformer aux exigences du présent règlement, lorsque la demande de normalisation n'a été acceptée par aucune des organisations européennes de normalisation, ou lorsque les normes harmonisées pertinentes ne répondent pas suffisamment aux préoccupations en matière de droits fondamentaux, ou lorsque les normes harmonisées ne sont pas conformes à la demande, ou lorsque l'adoption d'une norme harmonisée appropriée accuse des retards. Lorsqu'un tel retard dans l'adoption d'une norme harmonisée est dû à la complexité technique de ladite norme, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes. Lorsqu'elle élabore des spécifications communes, la Commission est encouragée à coopérer avec des partenaires internationaux et des organismes internationaux de normalisation.

- (122) Il convient que, sans préjudice de l'utilisation de normes harmonisées et de spécifications communes, les fournisseurs d'un système d'IA à haut risque qui a été entraîné et testé avec des données reflétant le cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel il est destiné à être utilisé soient présumés comme se conformant à la mesure pertinente prévue au titre de l'exigence en matière de gouvernance des données énoncée dans le présent règlement. Sans préjudice des exigences liées à la robustesse et à l'exactitude énoncées dans le présent règlement, conformément à l'article 54, paragraphe 3, du règlement (UE) 2019/881, les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité en vertu dudit règlement et dont les références ont été publiées au *Journal officiel de l'Union européenne* devraient être présumés conformes aux exigences de cybersécurité du présent règlement dans la mesure où le certificat de cybersécurité ou la déclaration de conformité, ou des parties de ceux-ci, couvrent l'exigence de cybersécurité du présent règlement. Cet aspect demeure sans préjudice du caractère volontaire dudit schéma de cybersécurité.
- (123) Afin de garantir un niveau élevé de fiabilité des systèmes d'IA à haut risque, ces systèmes devraient être soumis à une évaluation de la conformité avant leur mise sur le marché ou leur mise en service.

- (124) Afin de réduire au minimum la charge pesant sur les opérateurs et d'éviter les éventuels doubles emplois, la conformité avec les exigences du présent règlement des systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation existante de l'Union fondée sur le nouveau cadre législatif devrait être évaluée dans le cadre de l'évaluation de la conformité déjà prévue en vertu de cette législation. L'applicabilité des exigences du présent règlement ne devrait donc pas avoir d'incidence sur la logique, la méthode ou la structure générale propres à l'évaluation de la conformité au titre de la législation d'harmonisation de l'Union pertinente.
- (125) Compte tenu de la complexité des systèmes d'IA à haut risque et des risques qui y sont associés, il importe d'élaborer une procédure d'évaluation de la conformité adéquat faisant intervenir les organismes notifiés pour ces systèmes, dite "évaluation de conformité par un tiers". Toutefois, étant donné l'expérience actuelle des organismes professionnels de certification avant mise sur le marché dans le domaine de la sécurité des produits et de la nature différente des risques encourus, il convient de limiter, au moins dans une phase initiale d'application du présent règlement, le champ d'application des évaluations de la conformité réalisées par un tiers aux systèmes d'IA à haut risque autres que ceux liés à des produits. Par conséquent, l'évaluation de la conformité de ces systèmes devrait en règle générale être réalisée par le fournisseur sous sa propre responsabilité, à la seule exception des systèmes d'IA destinés à être utilisés à des fins de biométrie.

- (126) Afin de procéder à des évaluations de la conformité par un tiers lorsque cela est nécessaire, les organismes notifiés devraient être notifiés en vertu du présent règlement par les autorités nationales compétentes, sous réserve qu'ils satisfassent à un ensemble d'exigences portant en particulier sur leur indépendance, leur compétence, l'absence de conflits d'intérêts et les exigences appropriées en matière de cybersécurité. La notification de ces organismes devrait être envoyée par les autorités nationales compétentes à la Commission et aux autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission, conformément à l'annexe I, article R23, de la décision n° 768/2008/CE.
- (127) Conformément aux engagements pris par l'Union au titre de l'accord de l'Organisation mondiale du commerce sur les obstacles techniques au commerce, il convient de faciliter la reconnaissance mutuelle des résultats des évaluations de la conformité produits par les organismes d'évaluation de la conformité compétents, indépendamment du territoire sur lequel ils sont établis, à condition que ces organismes d'évaluation de la conformité établis en vertu du droit d'un pays tiers satisfassent aux exigences applicables en vertu du présent règlement et que l'Union ait conclu un accord en ce sens. Dans ce contexte, la Commission devrait étudier activement d'éventuels instruments internationaux à cette fin et, en particulier, œuvrer à la conclusion d'accords de reconnaissance mutuelle avec des pays tiers.

- (128) Conformément à la notion communément établie de modification substantielle pour les produits réglementés par la législation d'harmonisation de l'Union, chaque fois que survient une modification susceptible d'avoir une incidence sur la conformité d'un système d'IA à haut risque avec le présent règlement (par exemple, un changement de système d'exploitation ou d'architecture logicielle) ou que la destination du système change, il convient de considérer ledit système d'IA comme un nouveau système d'IA devant être soumis à nouvelle procédure d'évaluation de la conformité. Cependant, les changements intervenant sur l'algorithme et la performance de systèmes d'IA qui continuent à "apprendre" après avoir été mis sur le marché ou mis en service, à savoir l'adaptation automatique de la façon dont les fonctions sont exécutées, ne devraient pas constituer une modification substantielle, à condition que ces changements aient été prédéterminés par le fournisseur et évalués au moment de l'évaluation de la conformité.
- (129) Le marquage "CE" devrait être apposé sur les systèmes d'IA à haut risque pour indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement dans le marché intérieur. Pour les systèmes d'IA à haut risque intégrés à un produit, un marquage "CE" physique devrait être apposé, éventuellement complété par un marquage "CE" numérique. Pour les systèmes d'IA à haut risque fournis uniquement sous forme numérique, il convient d'utiliser un marquage "CE" numérique. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché ou à la mise en service de systèmes d'IA à haut risque qui satisfont aux exigences fixées dans le présent règlement et portent le marquage "CE".

- (130) Dans certaines conditions, la disponibilité rapide de technologies innovantes peut être cruciale pour la santé et la sécurité des personnes, pour la protection de l'environnement et la lutte contre le changement climatique et pour la société dans son ensemble. Il convient donc que, pour des motifs exceptionnels liés à la sécurité publique ou à la protection de la vie et de la santé des personnes physiques, à la protection de l'environnement et à la protection d'actifs industriels et d'infrastructures d'importance majeure, les autorités de surveillance du marché puissent autoriser la mise sur le marché ou la mise en service de systèmes d'IA qui n'ont pas fait l'objet d'une évaluation de la conformité. Dans des situations dûment justifiées, prévues dans le présent règlement, les autorités répressives ou les autorités de protection civile peuvent mettre en service un système d'IA à haut risque spécifique sans avoir obtenu l'autorisation de l'autorité de surveillance du marché, à condition que cette autorisation soit demandée sans retard injustifié pendant ou après l'utilisation.
- (131) Afin de faciliter les travaux de la Commission et des États membres dans le domaine de l'IA et d'accroître la transparence à l'égard du public, les fournisseurs de systèmes d'IA à haut risque autres que ceux liés à des produits relevant du champ d'application de la législation d'harmonisation existante de l'Union en la matière, ainsi que les fournisseurs qui considèrent qu'un système d'IA inscrit sur la liste des cas d'utilisation à haut risque dans une annexe du présent règlement n'est pas à haut risque sur la base d'une dérogation, devraient être tenus de s'enregistrer eux-mêmes et d'enregistrer les informations relatives à leur système d'IA dans une base de données de l'UE, qui sera établie et gérée par la Commission. Avant d'utiliser un système d'IA inscrit sur la liste des cas d'utilisation à haut risque dans une annexe du présent règlement, les déployeurs de systèmes d'IA à haut risque qui sont des autorités, des agences ou des organismes publics devraient s'enregistrer dans une telle base de données et sélectionner le système qu'ils envisagent d'utiliser.

Les autres déployeurs devraient être autorisés à le faire volontairement. Cette section de la base de données de l'UE devrait être accessible au public sans frais, et les informations qu'elle contient devraient être consultables grâce à une navigation aisée et être facilement compréhensibles et lisibles par machine. La base de données de l'UE devrait également être conviviale, par exemple en offrant des fonctionnalités de recherche, y compris par mots-clés, afin de permettre au grand public de trouver les informations pertinentes devant être transmises au moment de l'enregistrement des systèmes d'IA à haut risque et les informations sur le cas d'utilisation de systèmes d'IA à haut risque, énoncés dans une annexe du présent règlement, auquel les systèmes d'IA à haut risque correspondent. Toute modification substantielle de systèmes d'IA à haut risque devrait également être enregistrée dans la base de données de l'UE. En ce qui concerne les systèmes d'IA à haut risque dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, les obligations en matière d'enregistrement devraient être remplies dans une section non publique sécurisée de la base de données de l'UE. L'accès à la section non publique sécurisée devrait être strictement réservé à la Commission, ainsi qu'aux autorités de surveillance du marché pour ce qui est de la section nationale de cette base de données les concernant. Les systèmes d'IA à haut risque dans le domaine des infrastructures critiques ne devraient être enregistrés qu'au niveau national. La Commission devrait faire fonction de responsable du traitement pour la base de données de l'UE, conformément au règlement (UE) 2018/1725. Afin de garantir que la base de données de l'UE soit pleinement opérationnelle une fois déployée, la procédure de création de la base de données devrait prévoir le développement de spécifications fonctionnelles par la Commission et un rapport d'audit indépendant. La Commission devrait tenir compte des risques liés à la cybersécurité dans l'accomplissement de ses missions en tant que responsable du traitement des données dans la base de données de l'UE. Afin de maximiser la disponibilité et l'utilisation de la base de données de l'UE, y compris les informations mises à disposition par son intermédiaire, la base de données de l'UE devrait être conforme aux exigences prévues par la directive (UE) 2019/882.

- (132) Certains systèmes d'IA destinés à interagir avec des personnes physiques ou à générer du contenu peuvent présenter des risques spécifiques d'usurpation d'identité ou de tromperie, qu'ils soient ou non considérés comme étant à haut risque. Dans certaines circonstances, l'utilisation de ces systèmes devrait donc être soumise à des obligations de transparence spécifiques sans préjudice des exigences et obligations relatives aux systèmes d'IA à haut risque et sous réserve d'exemptions ciblées destinées à tenir compte des besoins spécifiques des activités répressives. En particulier, les personnes physiques devraient être avisées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation. Lors de la mise en œuvre de cette obligation, les caractéristiques des personnes physiques appartenant à des groupes vulnérables en raison de leur âge ou d'un handicap devraient être prises en compte dans la mesure où le système d'IA est destiné à interagir également avec ces groupes. En outre, les personnes physiques devraient être mises au courant lorsqu'elles sont exposées à des systèmes d'IA qui, en traitant leurs données biométriques, peuvent identifier ou déduire les émotions ou intentions de ces personnes ou les affecter à des catégories spécifiques. Ces catégories spécifiques peuvent avoir trait à des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits personnels, l'origine ethnique, les préférences et les intérêts personnels. Ces informations et notifications devraient être fournies dans des formats accessibles aux personnes handicapées.

(133) Divers systèmes d'IA peuvent générer de grandes quantités de contenu de synthèse qu'il devient de plus en plus difficile pour les êtres humains de distinguer du contenu authentique généré par des humains. La large disponibilité et les capacités croissantes de ces systèmes ont des conséquences importantes sur l'intégrité de l'écosystème informationnel et la confiance en celui-ci, ce qui pose de nouveaux risques de désinformation et de manipulation à grande échelle, de fraude, d'usurpation d'identité et de tromperie des consommateurs. Compte tenu de ces effets, du rythme rapide de l'évolution technologique et de la nécessité de nouvelles méthodes et techniques pour déterminer l'origine des informations, il convient d'exiger que les fournisseurs de ces systèmes intègrent des solutions techniques permettant le marquage dans un format lisible par machine et la détection du fait que les sorties ont été générées ou manipulées par un système d'IA, et non par un être humain. De telles techniques et méthodes devraient être aussi fiables, interopérables, efficaces et solides que la technologie le permet, et tenir compte des techniques disponibles ou d'une combinaison de ces techniques, telles que les filigranes, les identifications de métadonnées, les méthodes cryptographiques permettant de prouver la provenance et l'authenticité du contenu, les méthodes d'enregistrement, les empreintes digitales ou d'autres techniques, selon qu'il convient. Lorsqu'ils mettent en œuvre cette obligation, les fournisseurs devraient également tenir compte des spécificités et des limites des différents types de contenu, ainsi que des évolutions technologiques et du marché pertinentes dans le domaine, tels qu'elles ressortent de l'état de la technique généralement reconnu. Ces techniques et méthodes peuvent être mises en œuvre au niveau du système d'IA ou au niveau du modèle d'IA, y compris pour les modèles d'IA à usage général qui génèrent du contenu, ce qui facilitera l'accomplissement de cette obligation par le fournisseur en aval du système d'IA. Dans un souci de proportionnalité, il convient d'envisager que cette obligation de marquage ne s'applique pas aux systèmes d'IA qui remplissent une fonction d'assistance pour la mise en forme standard ou les systèmes d'IA qui ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique.

- (134) Outre les solutions techniques utilisées par les fournisseurs du système, les déployeurs qui se servent d'un système d'IA pour générer ou manipuler des images ou des contenus audio ou vidéo présentant une ressemblance sensible avec des personnes, des objets, des lieux, des entités ou des événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques (hypertrucages), devraient aussi déclarer de manière claire et reconnaissable que le contenu a été créé ou manipulé par une IA en étiquetant les sorties d'IA en conséquence et en mentionnant son origine artificielle. Le respect de cette obligation de transparence ne devrait pas être interprété comme indiquant que l'utilisation du système d'IA ou des sorties qu'il génère entrave le droit à la liberté d'expression et le droit à la liberté des arts et des sciences garantis par la Charte, en particulier lorsque le contenu fait partie d'un travail ou d'un programme manifestement créatif, satirique, artistique; de fiction ou analogue, sous réserve de garanties appropriées pour les droits et libertés de tiers. Dans ces cas, l'obligation de transparence s'appliquant aux hypertrucages au titre du présent règlement se limite à la divulgation de l'existence de tels contenus générés ou manipulés, d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre, y compris son exploitation et son utilisation normales, tout en préservant l'utilité et la qualité de l'œuvre. En outre, il convient d'envisager une obligation d'information similaire en ce qui concerne le texte généré ou manipulé par l'IA dans la mesure où celui-ci est publié dans le but d'informer le public sur des questions d'intérêt public, à moins que le contenu généré par l'IA n'ait fait l'objet d'un processus d'examen humain ou de contrôle éditorial et qu'une personne physique ou morale assume la responsabilité éditoriale pour la publication du contenu.

- (135) Sans préjudice de la nature obligatoire et de la pleine applicabilité des obligations de transparence, la Commission peut également encourager et faciliter l'élaboration de codes de bonne pratique au niveau de l'Union afin de faciliter la mise en œuvre effective des obligations relatives à la détection et à l'étiquetage des contenus générés ou manipulés par une IA, y compris pour favoriser des modalités pratiques visant, selon qu'il convient, à rendre les mécanismes de détection accessibles et à faciliter la coopération avec d'autres acteurs tout au long de la chaîne de valeur, à diffuser les contenus ou à vérifier leur authenticité et leur provenance pour permettre au public de reconnaître efficacement les contenus générés par l'IA.
- (136) Les obligations incombant aux fournisseurs et aux dépoyeurs de certains systèmes d'IA au titre du présent règlement afin de permettre la détection et la mention du fait que les sorties de ces systèmes sont générées ou manipulées par une IA revêtent une importance particulière pour faciliter la mise en œuvre effective du règlement (UE) 2022/2065. Cela vaut en particulier pour les obligations incombant aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne consistant à recenser et à atténuer les risques systémiques susceptibles de découler de la diffusion de contenus qui ont été générés ou manipulés par une IA, en particulier le risque d'effets négatifs réels ou prévisibles sur les processus démocratiques, le débat public et les processus électoraux, notamment par le biais de la désinformation. L'exigence relative à l'étiquetage des contenus générés par des systèmes d'IA au titre du présent règlement est sans préjudice de l'obligation prévue à l'article 16, paragraphe 6, du règlement (UE) 2022/2065 imposant aux fournisseurs de services d'hébergement de traiter les signalements de contenus illégaux qu'ils reçoivent au titre de l'article 16, paragraphe 1, dudit règlement, et elle ne devrait pas influencer l'évaluation et la décision quant à l'illégalité du contenu en question. Cette évaluation ne devrait être effectuée qu'au regard des règles régissant la légalité du contenu.

- (137) Le respect des obligations de transparence applicables aux systèmes d'IA relevant du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système d'IA ou de ses sorties est licite en vertu du présent règlement ou d'autres actes législatifs de l'Union et des États membres et devrait être sans préjudice d'autres obligations de transparence pour les déployeurs de systèmes d'IA prévues par le droit de l'Union ou le droit national.
- (138) L'IA est une famille de technologies en évolution rapide qui nécessite la mise en place d'un contrôle réglementaire et d'un espace sûr et contrôlé pour l'expérimentation, garantissant également une innovation responsable et l'intégration de garanties et de mesures d'atténuation des risques appropriées. Pour garantir un cadre juridique favorable à l'innovation, à l'épreuve du temps et résilient face aux perturbations, les États membres devraient veiller à ce que leurs autorités nationales compétentes mettent en place au moins un bac à sable réglementaire de l'IA au niveau national pour faciliter le développement et la mise à l'essai de systèmes d'IA innovants sous un contrôle réglementaire strict avant que ces systèmes ne soient mis sur le marché ou mis en service d'une autre manière. Les États membres pourraient également satisfaire à cette obligation en participant à des bacs à sable réglementaires déjà existants ou en établissant conjointement un bac à sable avec les autorités compétentes d'un ou de plusieurs États membres, pour autant que cette participation offre un niveau de couverture nationale équivalent pour les États membres participants. Les bacs à sable réglementaires de l'IA pourraient être mis en place sous forme physique, numérique ou hybride et admettre des produits tant physiques que numériques. Les autorités chargées de les mettre en place devraient également veiller à ce que les bacs à sable réglementaires de l'IA disposent des ressources appropriées pour assurer leur fonctionnement, y compris les ressources financières et humaines.

- (139) Les bacs à sable réglementaires de l'IA devraient avoir pour objectif de favoriser l'innovation dans le domaine de l'IA en créant un environnement contrôlé d'expérimentation et d'essai au stade du développement et de la précommercialisation afin de garantir la conformité des systèmes d'IA innovants avec le présent règlement et d'autres dispositions pertinentes du droit de l'Union et du droit national. De plus, les bacs à sable réglementaires de l'IA devraient viser à renforcer la sécurité juridique pour les innovateurs ainsi que le contrôle et la compréhension, par les autorités compétentes, des possibilités, des risques émergents et des conséquences de l'utilisation de l'IA, de faciliter l'apprentissage réglementaire pour les autorités et les entreprises, y compris en vue d'ajustements futurs du cadre juridique, de soutenir la coopération et l'échange de bonnes pratiques avec les autorités participant au bac à sable réglementaire de l'IA, et d'accélérer l'accès aux marchés, notamment en supprimant les obstacles pour les PME, y compris les jeunes pousses. Les bacs à sable réglementaires de l'IA devraient être largement disponibles dans toute l'Union, et il convient de prêter une attention particulière à leur accessibilité pour les PME, y compris les jeunes pousses. La participation au bac à sable réglementaire de l'IA devrait se concentrer sur les questions qui créent une insécurité juridique pour les fournisseurs et les fournisseurs potentiels avant d'innover, d'expérimenter l'IA dans l'Union et de contribuer à un apprentissage réglementaire fondé sur des données probantes. La surveillance des systèmes d'IA dans le bac à sable réglementaire de l'IA devrait donc porter sur leur développement, leur entraînement, leur mise à l'essai et leur validation avant que les systèmes ne soient mis sur le marché ou mis en service, ainsi que sur la notion et la survenance de modifications substantielles susceptibles de nécessiter une nouvelle procédure d'évaluation de la conformité. Tout risque important recensé lors du développement et de la mise à l'essai de ces systèmes d'IA devrait donner lieu à des mesures d'atténuation adéquates et, à défaut, à la suspension du processus de développement et d'essai.

Au besoin, les autorités nationales compétentes mettant en place des bacs à sable réglementaires de l'IA devraient coopérer avec d'autres autorités concernées, y compris celles qui supervisent la protection des droits fondamentaux, et pourraient permettre la participation d'autres acteurs de l'écosystème de l'IA, tels que les organisations nationales ou européennes de normalisation, les organismes notifiés, les installations d'essai et d'expérimentation, les laboratoires de recherche et d'expérimentation, les pôles européens d'innovation numérique, ainsi que les parties prenantes et les organisations de la société civile concernées. Pour assurer une mise en œuvre uniforme dans toute l'Union et des économies d'échelle, il convient d'établir des règles communes pour la mise en place des bacs à sable réglementaires de l'IA ainsi qu'un cadre de coopération entre les autorités compétentes intervenant dans la surveillance des bacs à sable. Les bacs à sable réglementaires de l'IA établis en vertu du présent règlement devraient être sans préjudice d'autres actes législatifs autorisant la création d'autres bacs à sable en vue de garantir le respect de dispositions de droit autres que le présent règlement. Le cas échéant, les autorités compétentes concernées chargées de ces autres bacs à sable réglementaires devraient prendre en considération les avantages de l'utilisation de ces bacs à sable également aux fins d'assurer la conformité des systèmes d'IA avec le présent règlement. Sous réserve d'un accord entre les autorités nationales compétentes et les participants au bac à sable réglementaire de l'IA, il peut également être procédé à des essais en conditions réelles supervisés dans le cadre du bac à sable réglementaire de l'IA.

- (140) Le présent règlement devrait constituer la base juridique pour l'utilisation, par les fournisseurs et fournisseurs potentiels du bac à sable réglementaire de l'IA, des données à caractère personnel collectées à d'autres fins pour le développement de certains systèmes d'IA d'intérêt public dans le cadre du bac à sable réglementaire de l'IA, uniquement dans des conditions déterminées, conformément à l'article 6, paragraphe 4, et à l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et aux articles 5, 6 et 10 du règlement (UE) 2018/1725, et sans préjudice de l'article 4, paragraphe 2, et de l'article 10 de la directive (UE) 2016/680. Toutes les autres obligations des responsables du traitement et tous les autres droits des personnes concernées en vertu des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680 restent applicables. En particulier, le présent règlement ne devrait pas constituer une base juridique au sens de l'article 22, paragraphe 2, point b), du règlement (UE) 2016/679 et de l'article 24, paragraphe 2, point b), du règlement (UE) 2018/1725. Les fournisseurs et fournisseurs potentiels participant au bac à sable réglementaire de l'IA devraient prévoir des garanties appropriées et coopérer avec les autorités compétentes, notamment en suivant leurs orientations et en agissant rapidement et de bonne foi pour atténuer adéquatement tout risque important recensé pour la sécurité, la santé et les droits fondamentaux susceptible de survenir au cours du développement, de la mise à l'essai et de l'expérimentation dans ledit bac à sable.

- (141) Afin d'accélérer le processus de développement et la mise sur le marché des systèmes d'IA à haut risque énumérés dans une annexe du présent règlement, il importe que les fournisseurs ou fournisseurs potentiels de ces systèmes puissent également bénéficier d'un régime particulier pour soumettre ces systèmes à des essais en conditions réelles sans participer à un bac à sable réglementaire de l'IA. Toutefois, dans de tels cas, compte tenu des conséquences possibles de ces essais sur des personnes physiques, il convient de veiller à ce que le présent règlement introduise des garanties et des conditions appropriées et suffisantes pour les fournisseurs ou fournisseurs potentiels. Ces garanties devraient comprendre, entre autres, une demande de consentement éclairé de la part des personnes physiques pour participer à des essais en conditions réelles, sauf en ce qui concerne les services répressifs lorsque la recherche d'un consentement éclairé empêcherait que le système d'IA ne soit mis à l'essai. Le consentement des participants à la participation à ces essais au titre du présent règlement est distinct et sans préjudice du consentement des personnes concernées au traitement de leurs données à caractère personnel en vertu de la législation applicable en matière de protection des données.

Il importe également important de réduire les risques au minimum et de permettre aux autorités compétentes d'exercer un contrôle et, par conséquent, d'exiger des fournisseurs potentiels qu'ils disposent d'un plan d'essais en conditions réelles présenté à l'autorité de surveillance du marché compétente, d'enregistrer les essais dans des sections spécifiques de la base de données de l'UE, sous réserve de quelques exceptions limitées, de fixer des limitations de la période pendant laquelle les essais peuvent être menés et d'exiger des garanties supplémentaires pour les personnes appartenant à certains groupes vulnérables, ainsi qu'un accord écrit définissant les rôles et les responsabilités des fournisseurs potentiels et des déployeurs et établissant un contrôle effectif par le personnel compétent participant aux essais en conditions réelles. En outre, il convient d'envisager des garanties supplémentaires pour veiller à ce que les prédictions, recommandations ou décisions d'un système d'IA puissent être infirmées et ignorées de manière effective et à ce que les données à caractère personnel soient protégées et supprimées lorsque les personnes concernées ont retiré leur consentement à participer aux essais, sans qu'il soit porté atteinte aux droits dont elles disposent en tant que personnes concernées en vertu du droit de l'Union en matière de protection des données. En ce qui concerne le transfert de données, il convient en outre d'envisager que les données collectées et traitées aux fins des essais en conditions réelles ne soient transférées vers des pays tiers que lorsque des garanties appropriées et applicables en vertu du droit de l'Union sont en place, en particulier conformément aux bases pour le transfert de données à caractère personnel prévues par le droit de l'Union en matière de protection des données, et que des garanties appropriées soient mises en place pour les données à caractère non personnel conformément au droit de l'Union, notamment les règlements (UE) 2022/868⁴² et (UE) 2023/2854⁴³ du Parlement européen et du Conseil.

⁴² Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).

⁴³ Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

- (142) Afin de veiller à ce que l'IA engendre des résultats bénéfiques sur le plan social et environnemental, les États membres sont encouragés à soutenir et à promouvoir la recherche et le développement de solutions d'IA propices à tels résultats, telles que des solutions fondées sur l'IA destinées à renforcer l'accessibilité pour les personnes handicapées, à réduire les inégalités socio-économiques ou à atteindre les objectifs environnementaux, en y affectant des ressources suffisantes, y compris des financements publics et de l'Union, et, lorsqu'il convient et pour autant que les critères d'éligibilité et de sélection soient remplis, en envisageant des projets spécifiques qui poursuivent ces objectifs. Ces projets devraient être fondés sur le principe d'une coopération interdisciplinaire entre les développeurs d'IA, les experts en matière d'inégalité et de non-discrimination, d'accessibilité, de droits des consommateurs, de droits environnementaux et numériques, ainsi que les universitaires.

(143) Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des PME, y compris les jeunes pousses, qui sont des fournisseurs ou des déployeurs de systèmes d'IA bénéficient d'une attention particulière. À cette fin, les États membres devraient prendre des initiatives à l'intention de ces opérateurs, notamment en matière de sensibilisation et de communication d'informations. Les États membres devraient fournir aux PME, y compris les jeunes pousses, qui ont leur siège social ou une succursale dans l'Union un accès prioritaire aux bacs à sable réglementaires de l'IA, à condition qu'elles remplissent les conditions d'éligibilité et les critères de sélection et sans exclure que d'autres fournisseurs et fournisseurs potentiels accèdent aux bacs à sable pour autant que les mêmes conditions et critères soient remplis. Les États membres devraient utiliser les canaux de communication existants, et en établissent de nouveaux s'il y a lieu, avec les PME, y compris les jeunes pousses, les déployeurs, d'autres innovateurs et, le cas échéant, les autorités publiques locales afin de soutenir les PME tout au long de leur trajectoire de développement en leur fournissant des orientations et en répondant à leurs questions concernant la mise en œuvre du présent règlement. Le cas échéant, ces canaux devraient collaborer pour créer des synergies et assurer la cohérence des orientations fournies aux PME, y compris les jeunes pousses, et aux déployeurs. En outre, les États membres devraient faciliter la participation des PME et d'autres parties concernées aux processus d'élaboration de la normalisation. Par ailleurs, les intérêts et les besoins spécifiques des fournisseurs qui sont des PME, y compris des jeunes pousses, devraient être pris en considération lorsque les organismes notifiés fixent les redevances d'évaluation de la conformité. La Commission devrait évaluer régulièrement les coûts de certification et de mise en conformité pour les PME, y compris les jeunes pousses, en menant des consultations transparentes, et devrait collaborer avec les États membres pour réduire ces coûts.

Par exemple, les frais de traduction liés à la documentation obligatoire et à la communication avec les autorités peuvent représenter un coût important pour les fournisseurs et d'autres opérateurs, en particulier pour ceux de plus petite envergure. Les États membres devraient éventuellement veiller à ce qu'une des langues qu'ils choisissent et acceptent pour la documentation pertinente des fournisseurs et pour la communication avec les opérateurs soit une langue comprise par le plus grand nombre possible de déployeurs transfrontières. Afin de répondre aux besoins spécifiques des PME, y compris les jeunes pousses, la Commission devrait fournir des modèles normalisés pour les domaines qui relèvent du présent règlement, sur demande du Comité IA. En outre, la Commission devrait compléter les efforts déployés par les États membres en mettant en place une plateforme d'information unique présentant des informations facilement exploitables concernant le présent règlement à l'intention de tous les fournisseurs et déployeurs, en organisant des campagnes de communication appropriées pour faire connaître les obligations découlant du présent règlement, et en évaluant et en promouvant la convergence des bonnes pratiques dans les procédures de passation de marchés publics relatifs aux systèmes d'IA. Les entreprises qui jusqu'à récemment relevaient des "petites entreprises" au sens de l'annexe à la recommandation 2003/361/CE de la Commission⁴⁴ devraient avoir accès à ces mesures de soutien, étant donné que ces nouvelles moyennes entreprises peuvent parfois manquer des ressources juridiques et de la formation nécessaires pour avoir une bonne compréhension du présent règlement et en respecter les dispositions.

⁴⁴ Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

- (144) Afin de promouvoir et de protéger l'innovation, la plateforme d'IA à la demande, ainsi que l'ensemble des programmes et projets de financement pertinents de l'Union, tels que le programme pour une Europe numérique et Horizon Europe, mis en œuvre par la Commission et les États membres au niveau national ou de l'Union, selon qu'il convient, devraient contribuer à la réalisation des objectifs du présent règlement.
- (145) Afin de réduire au minimum les risques pour la mise en œuvre résultant du manque de connaissances et d'expertise sur le marché, ainsi que de faciliter la mise en conformité des fournisseurs, en particulier des PME, y compris les jeunes pousses, et des organismes notifiés avec les obligations qui leur incombent au titre du présent règlement, la plateforme d'IA à la demande, les pôles européens d'innovation numérique et les installations d'expérimentation et d'essai mis en place par la Commission et les États membres au niveau de l'Union ou au niveau national devraient contribuer à la mise en œuvre du présent règlement. Dans le cadre de leurs missions et domaines de compétence respectifs, la plateforme d'IA à la demande, les pôles européens d'innovation numérique et les installations d'expérimentation et d'essai sont notamment en mesure d'apporter un soutien technique et scientifique aux fournisseurs et aux organismes notifiés.

- (146) En outre, au vu de la très petite taille de certains opérateurs et afin d'assurer la proportionnalité en ce qui concerne les coûts de l'innovation, il convient de permettre aux microentreprises de satisfaire à l'une des obligations les plus coûteuses, à savoir celle de mettre en place un système de gestion de la qualité, d'une manière simplifiée qui réduirait la charge administrative et les coûts pour ces entreprises sans affecter le niveau de protection et la nécessité de se conformer aux exigences applicables aux systèmes d'IA à haut risque. La Commission devrait élaborer des lignes directrices pour préciser quels éléments du système de gestion de la qualité les microentreprises doivent respecter dans le système simplifié.
- (147) Il convient que la Commission facilite, dans la mesure du possible, l'accès aux installations d'expérimentation et d'essai pour les organismes, groupes ou laboratoires qui ont été créés ou accrédités en vertu d'une législation d'harmonisation de l'Union pertinente et qui accomplissent des tâches dans le cadre de l'évaluation de la conformité des produits ou dispositifs couverts par la législation d'harmonisation de l'Union en question. C'est en particulier le cas en ce qui concerne les groupes d'experts, les laboratoires spécialisés et les laboratoires de référence dans le domaine des dispositifs médicaux conformément aux règlements (UE) 2017/745 et (UE) 2017/746.

(148) Le présent règlement devrait établir un cadre de gouvernance qui permette à la fois de coordonner et de soutenir l'application du présent règlement au niveau national, ainsi que de renforcer les capacités au niveau de l'Union et d'intégrer les parties prenantes dans le domaine de l'IA. La mise en œuvre et le contrôle de l'application effectifs du présent règlement requièrent un cadre de gouvernance qui permette de coordonner et de renforcer l'expertise centrale au niveau de l'Union. Le Bureau de l'IA a été créé par voie d'une décision⁴⁵ de la Commission et a pour mission d'approfondir l'expertise et de renforcer les capacités de l'Union dans le domaine de l'IA ainsi que de contribuer à la mise en œuvre de la législation de l'Union sur l'IA. Les États membres devraient faciliter l'accomplissement des missions du Bureau de l'IA en vue de soutenir le développement de l'expertise de l'Union et des capacités au niveau de l'Union et de renforcer le fonctionnement du marché unique numérique. En outre, il convient d'établir un Comité IA composé de représentants des États membres, un groupe scientifique visant à intégrer la communauté scientifique et un forum consultatif visant à recueillir les contributions des parties concernées en vue de la mise en œuvre du présent règlement, au niveau de l'Union et au niveau national. Le développement de l'expertise et des capacités de l'Union devrait également consister à utiliser les ressources et l'expertise existantes, en particulier grâce à des synergies avec les structures établies dans le contexte de l'application au niveau de l'Union d'autres dispositions législatives et à des synergies avec des initiatives connexes au niveau de l'Union, telles que l'entreprise commune EuroHPC et les installations de mise à l'essai de l'IA et d'expérimentations relevant du programme pour une Europe numérique.

⁴⁵ Décision de la Commission du 24 janvier 2024 créant le Bureau européen de l'intelligence artificielle (C/2024/390).

(149) Afin de faciliter une mise en œuvre aisée, efficace et harmonisée du présent règlement, il convient de créer un Comité IA. Ce Comité IA devrait tenir compte des différents intérêts de l'écosystème de l'IA et être composé de représentants des États membres. Le Comité IA devrait être chargé d'un certain nombre de tâches consultatives, parmi lesquelles la formulation d'avis, de recommandations, de conseils ou la contribution à des orientations sur des questions liées à la mise en œuvre du présent règlement, y compris sur les questions relatives à l'exécution, les spécifications techniques ou les normes existantes concernant les exigences établies dans le présent règlement, et la fourniture de conseils à la Commission et aux États membres ainsi qu'à leurs autorités nationales compétentes sur des questions spécifiques liées à l'IA. Afin d'offrir une certaine souplesse aux États membres dans la désignation de leurs représentants au sein du Comité IA, ces représentants peuvent être toute personne appartenant à des entités publiques qui devraient avoir les compétences et les pouvoirs nécessaires pour faciliter la coordination au niveau national et contribuer à l'accomplissement des tâches du Comité IA. Le Comité IA devrait établir deux sous-groupes permanents chargés de fournir une plateforme de coopération et d'échange entre les autorités de surveillance du marché et les autorités notifiantes sur des questions liées respectivement à la surveillance du marché et aux organismes notifiés. Le sous-groupe permanent pour la surveillance du marché devrait agir au titre de groupe de coopération administrative (ADCO) pour le présent règlement au sens de l'article 30 du règlement (UE) 2019/1020. Conformément à l'article 33 dudit règlement, la Commission devrait apporter son soutien aux activités du sous-groupe permanent en procédant à des évaluations ou à des études du marché, en particulier en vue de recenser les aspects du présent règlement appelant une coordination particulière urgente entre les autorités de surveillance du marché. Le Comité IA peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le Comité IA devrait également coopérer, lorsqu'il y a lieu, avec les organes, groupes d'experts et réseaux compétents de l'Union actifs dans le contexte de dispositions législatives pertinentes de l'Union, notamment ceux qui agissent au titre de la législation applicable de l'Union en matière de données, et de produits et services numériques.

- (150) En vue d'assurer la participation des parties prenantes à la mise en œuvre et à l'application du présent règlement, il convient d'établir un forum consultatif chargé de conseiller le Comité IA et la Commission et de leur fournir une expertise technique. Afin d'assurer une représentation diversifiée et équilibrée des parties prenantes tenant compte des différents intérêts commerciaux et non commerciaux et, au sein de la catégorie des intérêts commerciaux, eu égard aux PME et autres entreprises, le forum consultatif devrait être composé, entre autres, de représentants du secteur, des jeunes pousses, des PME, du milieu universitaire, de la société civile, y compris les partenaires sociaux, ainsi que de l'Agence des droits fondamentaux, de l'ENISA, du Comité européen de normalisation (CEN), du Comité européen de normalisation électrotechnique (CENELEC) et de l'Institut européen de normalisation des télécommunications (ETSI).
- (151) Afin de soutenir la mise en œuvre et le contrôle du respect du présent règlement, en particulier les activités de suivi du Bureau de l'IA concernant les modèles d'IA à usage général, il convient d'établir un groupe scientifique composé d'experts indépendants. Les experts indépendants constituant le groupe scientifique devraient être choisis en fonction de leur expertise à la pointe des connaissances scientifiques ou techniques dans le domaine de l'IA. Ils devraient s'acquitter de leurs tâches avec impartialité et objectivité et veiller à la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités. Afin de permettre le renforcement des capacités nationales nécessaires au contrôle effectif du respect du présent règlement, les États membres devraient être en mesure de solliciter l'aide de la réserve d'experts constituant le groupe scientifique pour leurs activités répressives.

- (152) Afin de soutenir un contrôle de l'application adéquat en ce qui concerne les systèmes d'IA et de renforcer les capacités des États membres, il convient de créer et de mettre à la disposition des États membres des structures de soutien de l'Union pour les essais en matière d'IA.
- (153) Les États membres jouent un rôle clé dans l'application et le contrôle du respect du présent règlement. À cet égard, chaque État membre devrait désigner au moins une autorité notifiante et au moins une autorité de surveillance du marché en tant qu'autorités nationales compétentes chargées de contrôler l'application et la mise en œuvre du présent règlement. Les États membres peuvent décider de désigner une entité publique, quel qu'en soit le type, qui soit chargée d'exécuter les tâches des autorités nationales compétentes au sens du présent règlement, en fonction de leurs caractéristiques et besoins organisationnels nationaux spécifiques. Afin d'accroître l'efficacité de l'organisation du côté des États membres et de définir un point de contact unique avec le public et les homologues au niveau des États membres et de l'Union, chaque État membre devrait désigner une autorité de surveillance du marché pour tenir le rôle de point de contact unique.
- (154) Les autorités nationales compétentes devraient exercer leurs pouvoirs de manière indépendante, impartiale et sans parti pris, afin de préserver les principes d'objectivité de leurs activités et de leurs tâches et d'assurer l'application et la mise en œuvre du présent règlement. Les membres de ces autorités devraient s'abstenir de toute action incompatible avec leurs fonctions et devraient être soumis aux règles de confidentialité prévues par le présent règlement.

- (155) Afin de veiller à ce que les fournisseurs de systèmes d'IA à haut risque puissent prendre en considération l'expérience acquise dans l'utilisation de systèmes d'IA à haut risque pour améliorer leurs systèmes et le processus de conception et de développement, ou qu'ils puissent prendre d'éventuelles mesures correctives en temps utile, tous les fournisseurs devraient avoir mis en place un système de surveillance après commercialisation. Le cas échéant, la surveillance après commercialisation devrait comprendre une analyse de l'interaction avec d'autres systèmes d'IA, y compris d'autres dispositifs et logiciels. La surveillance après commercialisation ne devrait pas couvrir les données opérationnelles sensibles des utilisateurs de systèmes d'IA qui sont des autorités répressives. Ce système est aussi essentiel pour garantir que les risques potentiels découlant des systèmes d'IA qui continuent à "apprendre" après avoir été mis sur le marché ou mis en service puissent être traités plus efficacement et en temps utile. Dans ce contexte, les fournisseurs devraient également être tenus de mettre en place un système pour signaler aux autorités compétentes tout incident grave résultant de l'utilisation de leurs systèmes d'IA, à savoir un incident ou un dysfonctionnement entraînant la mort ou une atteinte grave à la santé, une perturbation grave et irréversible de la gestion et de l'exploitation des infrastructures critiques, des infractions aux obligations découlant du droit de l'Union visant à protéger les droits fondamentaux ou une atteinte grave aux biens ou à l'environnement.

(156) Afin de garantir un contrôle approprié et efficace du respect des exigences et obligations énoncées par le présent règlement, qui fait partie de la législation d'harmonisation de l'Union, le système de surveillance du marché et de mise en conformité des produits établi par le règlement (UE) 2019/1020 devrait s'appliquer dans son intégralité. Les autorités de surveillance du marché désignées en vertu du présent règlement devraient disposer de tous les pouvoirs d'exécution prévus par le présent règlement et par le règlement (UE) 2019/1020, et elles devraient exercer leurs pouvoirs et s'acquitter de leurs tâches de manière indépendante, impartiale et sans parti pris. Bien que la majorité des systèmes d'IA ne fassent pas l'objet d'exigences et obligations particulières au titre du présent règlement, les autorités de surveillance du marché peuvent prendre des mesures à l'égard de tous les systèmes d'IA lorsqu'ils présentent un risque conformément au présent règlement. En raison de la nature spécifique des institutions, agences et organes de l'Union relevant du champ d'application du présent règlement, il convient de désigner le Contrôleur européen de la protection des données comme autorité compétente pour la surveillance du marché en ce qui les concerne. Cela devrait être sans préjudice de la désignation des autorités nationales compétentes par les États membres. Les activités de surveillance du marché ne devraient pas affecter la capacité des entités surveillées à s'acquitter de leurs tâches de manière indépendante, lorsque cette indépendance constitue une exigence du droit de l'Union.

- (157) Le présent règlement est sans préjudice des compétences, des tâches, des pouvoirs et de l'indépendance des autorités ou organismes publics nationaux compétents qui contrôlent l'application du droit de l'Union en matière de protection des droits fondamentaux, y compris les organismes chargés des questions d'égalité et les autorités de protection des données. Lorsque leur mandat l'exige, ces autorités ou organismes publics nationaux devraient également avoir accès à toute documentation créée en vertu du présent règlement. Une procédure de sauvegarde spécifique devrait être mise en place pour garantir une application adéquate et en temps utile opposable aux systèmes d'IA présentant un risque pour la santé, la sécurité et les droits fondamentaux. La procédure applicable à ces systèmes d'IA présentant un risque devrait être appliquée aux systèmes d'IA à haut risque présentant un risque, aux systèmes interdits qui ont été mis sur le marché, mis en service ou utilisés en violation des interdictions concernant des pratiques définies par le présent règlement, et aux systèmes d'IA qui ont été mis à disposition en violation des exigences de transparence énoncées dans le présent règlement et qui présentent un risque.

(158) Le droit de l'Union en matière de services financiers comprend des règles et des exigences en matière de gouvernance interne et de gestion des risques qui sont applicables aux établissements financiers réglementés dans le cadre de la fourniture de ces services, y compris lorsqu'ils font usage de systèmes d'IA. Afin d'assurer la cohérence de l'application et du contrôle du respect des obligations découlant du présent règlement et des règles et exigences pertinentes prévues par les actes juridiques de l'Union sur les services financiers, les autorités compétentes chargées de la surveillance et du contrôle de l'application de ces actes juridiques, en particulier les autorités compétentes au sens du règlement (UE) n° 575/2013 du Parlement européen et du Conseil⁴⁶ et des directives 2008/48/CE⁴⁷, 2009/138/CE⁴⁸, 2013/36/UE⁴⁹, 2014/17/UE⁵⁰ et (UE) 2016/97⁵¹ du Parlement européen et du Conseil, devraient être désignées, dans les limites de leurs compétences respectives, comme les autorités compétentes aux fins de la surveillance de la mise en œuvre du présent règlement, y compris pour les activités de surveillance du marché, en ce qui concerne les systèmes d'IA fournis ou utilisés par des établissements financiers réglementés et surveillés, à moins que les États membres ne décident de désigner une autre autorité pour remplir ces tâches de surveillance du marché.

⁴⁶ Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).

⁴⁷ Directive 2008/48/CE du Parlement européen et du Conseil du 23 avril 2008 concernant les contrats de crédit aux consommateurs et abrogeant la directive 87/102/CEE du Conseil (JO L 133 du 22.5.2008, p. 66).

⁴⁸ Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (JO L 335 du 17.12.2009, p. 1).

⁴⁹ Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

⁵⁰ Directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) n° 1093/2010 (JO L 60 du 28.2.2014, p. 34).

⁵¹ Directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances (JO L 26 du 2.2.2016, p. 19).

Ces autorités compétentes devraient disposer, en vertu du présent règlement et du règlement (UE) 2019/1020, de tous les pouvoirs nécessaires pour faire respecter les exigences et obligations du présent règlement, y compris le pouvoir d'effectuer des activités de surveillance du marché ex post qui peuvent être intégrées, le cas échéant, dans leurs mécanismes et procédures de surveillance existants au titre du droit de l'Union en matière de services financiers. Il convient d'envisager que, lorsqu'elles agissent en tant qu'autorités de surveillance du marché au titre du présent règlement, les autorités nationales responsables de la surveillance des établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) n° 1024/2013 du Conseil⁵², doivent communiquer sans délai à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt pour les missions de surveillance prudentielle de la Banque centrale européenne telles qu'elles sont définies dans ledit règlement. Pour renforcer encore la cohérence entre le présent règlement et les règles applicables aux établissements de crédit régis par la directive 2013/36/UE, il convient aussi d'intégrer certaines des obligations procédurales des fournisseurs en ce qui concerne la gestion des risques, la surveillance après commercialisation et la documentation dans les obligations et procédures existantes au titre de la directive 2013/36/UE. Afin d'éviter les chevauchements, des dérogations limitées devraient aussi être envisagées en ce qui concerne le système de gestion de la qualité des fournisseurs et l'obligation de suivi imposée aux dépoyeurs de systèmes d'IA à haut risque dans la mesure où les dispositions y afférentes s'appliquent aux établissements de crédit régis par la directive 2013/36/UE. Le même régime devrait s'appliquer aux entreprises d'assurance et de réassurance et aux sociétés holding d'assurance relevant de la directive 2009/138/CE, aux intermédiaires d'assurance relevant de la directive (UE) 2016/97, ainsi qu'aux autres types d'établissements financiers soumis à des exigences en matière de gouvernance, de dispositifs ou de processus internes établis en vertu des dispositions pertinentes du droit de l'Union en matière de services financiers afin d'assurer la cohérence et l'égalité de traitement dans le secteur financier.

⁵² Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

- (159) Chaque autorité de surveillance du marché chargée des systèmes d'IA à haut risque dans le domaine de la biométrie énumérés dans une annexe du présent règlement, dans la mesure où ces systèmes sont utilisés à des fins liées aux activités répressives, à la migration, à l'asile et à la gestion des contrôles aux frontières ou à l'administration de la justice et aux processus démocratiques, devrait disposer de pouvoirs effectifs en matière d'enquête et de mesures correctives, y compris au minimum le pouvoir d'obtenir l'accès à toutes les données à caractère personnel traitées et à toutes les informations nécessaires à l'accomplissement de ses tâches. Les autorités de surveillance du marché devraient être en mesure d'exercer leurs pouvoirs en toute indépendance. Toute restriction de leur accès à des données opérationnelles sensibles au titre du présent règlement devrait être sans préjudice des pouvoirs qui leur sont conférés par la directive (UE) 2016/680. Aucune exclusion concernant la divulgation de données aux autorités nationales chargées de la protection des données au titre du présent règlement ne devrait avoir d'incidence sur les pouvoirs actuels ou futurs de ces autorités au-delà du champ d'application du présent règlement.
- (160) Les autorités de surveillance du marché et la Commission devraient être en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener par les autorités de surveillance du marché ou par les autorités de surveillance du marché conjointement avec la Commission, visant à promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser et de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont recensés comme présentant un risque grave dans au moins deux États membres. Les activités conjointes visant à promouvoir le respect de la législation devraient être menées conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA devrait assurer la coordination centrale des enquêtes conjointes.

- (161) Il est nécessaire de clarifier les responsabilités et les compétences au niveau de l'Union et au niveau national en ce qui concerne les systèmes d'IA qui reposent sur des modèles d'IA à usage général. Afin d'éviter les chevauchements de compétences, lorsqu'un système est fondé sur un modèle d'IA à usage général et que le modèle et le système sont fournis par le même fournisseur, la surveillance devrait avoir lieu au niveau de l'Union par l'intermédiaire du Bureau de l'IA, qui devrait disposer à cette fin des pouvoirs d'une autorité de surveillance du marché au sens du règlement (UE) 2019/1020. Dans tous les autres cas, les autorités nationales de surveillance du marché demeurent chargées de la surveillance des systèmes d'IA. Toutefois, pour les systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque, les autorités de surveillance du marché devraient coopérer avec le Bureau de l'IA pour mener les évaluations de la conformité, et informer le Comité IA et les autres autorités de surveillance du marché en conséquence. En outre, toute autorité de surveillance du marché devrait être en mesure de solliciter l'assistance du Bureau de l'IA lorsqu'elle n'est pas en mesure de conclure une enquête sur un système d'IA à haut risque parce qu'elle ne peut accéder à certaines informations liées au modèle d'IA à usage général sur lequel repose ce système. Dans de tels cas, la procédure relative à l'assistance mutuelle pour les cas transfrontières prévue au chapitre VI du règlement (UE) 2019/1020 devrait s'appliquer mutatis mutandis.

- (162) Afin de tirer le meilleur parti de l'expertise centralisée de l'Union et des synergies au niveau de l'Union, les pouvoirs de surveillance et de contrôle du respect des obligations incombant aux fournisseurs de modèles d'IA à usage général devraient relever de la compétence de la Commission. Le Bureau de l'IA devrait être en mesure de prendre toutes les mesures nécessaires pour contrôler la mise en œuvre effective du présent règlement en ce qui concerne les modèles d'IA à usage général. Il devrait être en mesure d'enquêter sur d'éventuelles infractions aux règles incombant aux fournisseurs de modèles d'IA à usage général, aussi bien de sa propre initiative, selon les résultats de ses activités de surveillance, ou sur demande des autorités de surveillance du marché conformément aux conditions prévues par le présent règlement. Afin de contribuer à une surveillance effective par le Bureau de l'IA, celui-ci devrait donner la possibilité aux fournisseurs en aval d'introduire des réclamations concernant d'éventuelles infractions aux règles relatives aux fournisseurs de modèles et systèmes d'IA à usage général.
- (163) En vue de compléter les systèmes de gouvernance des modèles d'IA à usage général, le groupe scientifique devrait soutenir les activités de surveillance du Bureau de l'IA et pourrait, dans certains cas, soumettre au Bureau de l'IA des alertes qualifiées qui déclenchent des mesures de suivi telles que des enquêtes. Cela devrait être le cas lorsque le groupe scientifique a des raisons de soupçonner qu'un modèle d'IA à usage général présente un risque concret et identifiable au niveau de l'Union. Cela devrait aussi être le cas lorsque le groupe scientifique a des raisons de soupçonner qu'un modèle d'IA à usage général remplit les critères qui conduiraient à une classification en tant que modèle d'IA à usage général présentant un risque systémique. Afin que le groupe scientifique dispose des informations nécessaires à l'exécution de ces tâches, il devrait exister un mécanisme permettant au groupe scientifique de demander à la Commission d'exiger du fournisseur qu'il fournisse des documents ou des informations.

(164) Le Bureau de l'IA devrait être en mesure de prendre les mesures nécessaires pour contrôler la mise en œuvre effective et le respect des obligations incombant aux fournisseurs de modèles d'IA à usage général énoncées dans le présent règlement. Le Bureau de l'IA devrait être en mesure d'enquêter sur d'éventuelles infractions conformément aux pouvoirs qui lui sont conférés au titre du présent règlement, y compris en exigeant des documents et des informations, en réalisant des évaluations, ainsi qu'en exigeant que des mesures soient prises par les fournisseurs de modèles d'IA à usage général. Lors de la réalisation des évaluations, afin de tirer parti d'une expertise indépendante, le Bureau de l'IA devrait pouvoir faire appel à des experts indépendants pour réaliser les évaluations en son nom. Le respect des obligations devrait pouvoir être imposé, entre autres, par des demandes de prendre des mesures appropriées, y compris des mesures d'atténuation des risques dans le cas de risques systémiques recensés, ainsi qu'en restreignant la mise à disposition du modèle sur le marché, en le retirant ou en le rappelant. À titre de garantie, lorsque cela est nécessaire en sus des droits procéduraux prévus par le présent règlement, les fournisseurs de modèles d'IA à usage général devraient jouir des droits procéduraux prévus à l'article 18 du règlement (UE) 2019/1020, qui devraient s'appliquer mutatis mutandis, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

(165) Le développement de systèmes d'IA autres que les systèmes d'IA à haut risque dans le respect des exigences du présent règlement peut conduire à une plus large adoption d'une IA éthique et digne de confiance dans l'Union. Les fournisseurs de systèmes d'IA qui ne sont pas à haut risque devraient être encouragés à établir des codes de conduite, accompagnés de mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire de tout ou partie des exigences obligatoires applicables aux systèmes d'IA à haut risque, adaptés en fonction de la destination des systèmes et des risques plus faibles encourus et tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur, tels que les cartes modèles et les fiches de données. Les fournisseurs et, le cas échéant, les déployeurs de tous les systèmes d'IA, à haut risque ou non, et modèles d'IA devraient aussi être encouragés à appliquer sur une base volontaire des exigences supplémentaires liées, par exemple, aux éléments des lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance, à la durabilité environnementale, aux mesures relatives à la maîtrise de l'IA, à la conception et au développement inclusifs et diversifiés des systèmes d'IA, y compris en prêtant attention aux personnes vulnérables et à l'accessibilité pour les personnes handicapées, à la participation des parties prenantes avec la contribution, le cas échéant, de parties prenantes concernées telles que les organisations d'entreprises et de la société civile, le milieu universitaire, les organismes de recherche, les syndicats et les organisations de protection des consommateurs à la conception et au développement des systèmes d'IA, ainsi qu'à la diversité des équipes de développement, y compris l'équilibre hommes-femmes. Afin que les codes de conduite volontaires portent leurs effets, ils devraient s'appuyer sur des objectifs clairs et des indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs. Ils devraient également être élaborés de manière inclusive, selon qu'il convient, avec la participation des parties prenantes concernées telles que les organisations d'entreprises et de la société civile, le milieu universitaire, les organismes de recherche, les syndicats et les organisations de protection des consommateurs. La Commission peut élaborer des initiatives, y compris de nature sectorielle, pour faciliter la suppression des obstacles techniques entravant l'échange transfrontière de données pour le développement de l'IA, notamment en ce qui concerne l'infrastructure d'accès aux données et l'interopérabilité sémantique et technique des différents types de données.

- (166) Il importe que les systèmes d'IA liés à des produits qui ne sont pas à haut risque au titre du présent règlement et qui ne sont donc pas tenus d'être conformes aux exigences énoncées pour les systèmes d'IA à haut risque soient néanmoins sûrs lorsqu'ils sont mis sur le marché ou mis en service. Pour contribuer à cet objectif, l'application du règlement (UE) 2023/988 du Parlement européen et du Conseil⁵³ constituerait un filet de sécurité.
- (167) Afin d'assurer une coopération constructive et en toute confiance entre les autorités compétentes au niveau de l'Union et au niveau national, toutes les parties intervenant dans l'application du présent règlement devraient respecter la confidentialité des informations et des données obtenues dans le cadre de l'exécution de leurs tâches, conformément au droit de l'Union et au droit national. Elles devraient s'acquitter de leurs tâches et activités de manière à protéger, en particulier, les droits de propriété intellectuelle, les informations commerciales confidentielles et les secrets d'affaires, la mise en œuvre effective du présent règlement, les intérêts en matière de sécurité nationale et publique, l'intégrité des procédures pénales et administratives et l'intégrité des informations classifiées.

⁵³ Règlement (UE) 2023/988 du Parlement européen et du Conseil du 10 mai 2023 relatif à la sécurité générale des produits, modifiant le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil et la directive (UE) 2020/1828 du Parlement européen et du Conseil, et abrogeant la directive 2001/95/CE du Parlement européen et du Conseil et la directive 87/357/CEE du Conseil (JO L 135 du 23.5.2023, p. 1).

- (168) Le respect des dispositions du présent règlement devrait pouvoir être imposé au moyen de sanctions et d'autres mesures d'exécution. Les États membres devraient prendre toutes les mesures nécessaires pour que les dispositions du présent règlement soient mises en œuvre et, notamment, prévoir des sanctions effectives, proportionnées et dissuasives en cas de violation de ces dispositions, et dans le respect du principe non bis in idem. Afin de renforcer et d'harmoniser les sanctions administratives applicables en cas de violation du présent règlement, il convient d'établir le montant maximal pour la fixation des amendes administratives pour certaines infractions spécifiques. Pour évaluer le montant des amendes, les États membres devraient, dans chaque cas d'espèce, tenir compte de toutes les caractéristiques propres à la situation spécifique, en prenant notamment en considération la nature, la gravité et la durée de l'infraction et ses conséquences, ainsi que la taille du fournisseur, en particulier s'il s'agit d'une PME, y compris les jeunes pousses. Le Contrôleur européen de la protection des données devrait avoir le pouvoir d'infliger des amendes aux institutions, agences et organes de l'Union relevant du présent règlement.
- (169) Le respect des obligations incombant aux fournisseurs de modèles d'IA à usage général au titre du présent règlement devrait pouvoir être imposé, entre autres, au moyen d'amendes. À cette fin, des niveaux appropriés d'amendes devraient également être fixés pour les infractions à ces obligations, y compris le non-respect de mesures demandées par la Commission en vertu du présent règlement, sous réserve de délais de prescription appropriés conformément du principe de proportionnalité. Toutes les décisions prises par la Commission au titre du présent règlement sont soumises au contrôle de la Cour de justice de l'Union européenne conformément au traité sur le fonctionnement de l'Union européenne, y compris la compétence de pleine juridiction de la Cour de justice en ce qui concerne les sanctions en application de l'article 261 du traité sur le fonctionnement de l'Union européenne.

- (170) Le droit de l'Union et le droit national prévoient déjà des voies de recours effectives pour les personnes physiques et morales qui subissent une atteinte à leurs droits et libertés en raison de l'utilisation de systèmes d'IA. Sans préjudice de ces recours, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement devrait avoir le droit d'introduire une réclamation auprès de l'autorité de surveillance du marché concernée.
- (171) Les personnes concernées devraient avoir le droit d'obtenir une explication lorsque la décision d'un déployeur est principalement fondée sur les sorties de certains systèmes d'IA à haut risque qui relèvent du champ d'application du présent règlement et lorsque cette décision produit des effets juridiques ou cause un préjudice important de façon similaire à ces personnes d'une manière qu'elles considèrent comme ayant une incidence négative sur leur santé, leur sécurité ou leurs droits fondamentaux. Cette explication devrait être claire et pertinente, et constituer une base à partir de laquelle les personnes concernées peuvent exercer leurs droits. Le droit d'obtenir une explication ne devrait pas s'appliquer à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions découlent du droit de l'Union ou du droit national et ne devrait s'appliquer que dans la mesure où ce droit n'est pas déjà prévu par le droit de l'Union.
- (172) Les personnes agissant en tant que lanceurs d'alerte eu égard à des infractions au présent règlement devraient être protégées en vertu du droit de l'Union. La directive (UE) 2019/1937 du Parlement européen et du Conseil⁵⁴ devrait donc s'appliquer aux signalements d'infractions au présent règlement et à la protection des personnes signalant ces infractions.

⁵⁴ Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17).

(173) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission pour lui permettre de modifier les conditions dans lesquelles un système d'IA ne doit pas être considéré comme étant à haut risque, la liste des systèmes d'IA à haut risque, les dispositions relatives à la documentation technique, le contenu de la déclaration "UE" de conformité, les dispositions relatives aux procédures d'évaluation de la conformité, les dispositions établissant les systèmes d'IA à haut risque auxquels devrait s'appliquer la procédure d'évaluation de la conformité fondée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique, le seuil, les critères de référence et les indicateurs, y compris en complétant ces critères de référence et indicateurs, dans les règles de classification des modèles d'IA à usage général présentant un risque systémique, les critères de désignation des modèles d'IA à usage général présentant un risque systémique, la documentation technique destinée aux fournisseurs de modèles d'IA à usage général et les informations relatives à la transparence pour les fournisseurs de modèles d'IA à usage général. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer"⁵⁵. En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués.

⁵⁵ JO L 123 du 12.5.2016, p. 1.

- (174) Compte tenu de l'évolution rapide des technologies et de l'expertise technique requise aux fins de la bonne application du présent règlement, la Commission devrait évaluer et réexaminer le présent règlement au plus tard le ... [*cinq ans à compter de la date d'entrée en vigueur du présent règlement*] et tous les quatre ans par la suite, et faire rapport au Parlement européen et au Conseil. En outre, en tenant compte des conséquences sur le champ d'application du présent règlement, la Commission devrait procéder à une évaluation de la nécessité de modifier une fois par an la liste des systèmes d'IA à haut risque et la liste des pratiques interdites. En outre, au plus tard le ... [*quatre ans après l'entrée en vigueur du présent règlement*] et tous les quatre ans par la suite, la Commission devrait évaluer la nécessité de modifier les rubriques de la liste des domaines à haut risque figurant à l'annexe du présent règlement, les systèmes d'IA relevant des obligations de transparence, l'efficacité du système de surveillance et de gouvernance ainsi que l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, y compris la nécessité de mesures ou d'actions supplémentaires, et faire rapport au Parlement européen et au Conseil. Enfin, au plus tard le ... [*quatre ans à compter de la date d'entrée en vigueur du présent règlement*] et tous les trois ans par la suite, la Commission devrait évaluer l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées pour les systèmes d'IA à haut risque dans le cas des systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour de tels systèmes d'IA.

- (175) Afin de garantir des conditions uniformes de mise en œuvre du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil⁵⁶.
- (176) Étant donné que l'objectif du présent règlement, à savoir améliorer le fonctionnement du marché intérieur et promouvoir l'adoption d'une IA axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, y compris la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des dimensions et des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

⁵⁶ Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

- (177) Afin d'assurer la sécurité juridique, de veiller à ce que les opérateurs disposent d'une période d'adaptation appropriée et d'éviter toute perturbation du marché, y compris en assurant la continuité de l'utilisation des systèmes d'IA, il convient que le présent règlement s'applique aux systèmes d'IA à haut risque qui ont été mis sur le marché ou mis en service avant la date générale d'application de celui-ci, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leur conception ou de leur destination. Il convient de préciser qu'à cet égard, la notion d'importante modification devrait être comprise comme équivalente sur le fond à celle de modification substantielle, qui est utilisée uniquement en ce qui concerne les systèmes d'IA à haut risque au titre du présent règlement. À titre exceptionnel et compte tenu de l'obligation de rendre des comptes au public, les exploitants de systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe du présent règlement et les exploitants de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques devraient prendre les mesures nécessaires pour se conformer aux exigences du présent règlement, respectivement, d'ici à la fin de 2030 et au plus tard le ... *[six ans à compter de la date d'entrée en vigueur du présent règlement]*.
- (178) Les fournisseurs de systèmes d'IA à haut risque sont encouragés à commencer à se conformer, sur une base volontaire, aux obligations pertinentes du présent règlement dès la période transitoire.

(179) Le présent règlement devrait s'appliquer à partir du ... [*deux ans à compter de la date d'entrée en vigueur du présent règlement*]. Toutefois, compte tenu du risque inacceptable associé à certaines utilisations de l'IA, les interdictions ainsi que les dispositions générales du présent règlement devraient déjà s'appliquer à compter du ... [*six mois à compter de la date d'entrée en vigueur du présent règlement*]. Si le plein effet de ces interdictions découle de la mise en place de la gouvernance et du contrôle du respect du présent règlement, il importe d'anticiper l'application des interdictions afin de tenir compte des risques inacceptables et d'avoir un effet sur d'autres procédures, par exemple en droit civil. En outre, l'infrastructure liée à la gouvernance et au système d'évaluation de la conformité devrait être opérationnelle avant le ... [*deux ans à compter de la date d'entrée en vigueur du présent règlement*], et les dispositions relatives aux organismes notifiés et à la structure de gouvernance devraient donc s'appliquer à compter du ... [*douze mois à compter de la date d'entrée en vigueur du présent règlement*]. Compte tenu du rythme rapide des avancées technologiques et de l'adoption des modèles d'IA à usage général, les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient s'appliquer à compter du ... [*douze mois à compter de la date d'entrée en vigueur du présent règlement*]. Les codes de bonne pratique devraient être prêts au plus tard le ... [*neuf mois à compter de la date d'entrée en vigueur du présent règlement*] afin de permettre aux fournisseurs de démontrer leur conformité à temps. Le Bureau de l'IA devrait veiller à ce que les règles et procédures de classification soient à jour des évolutions technologiques. En outre, les États membres devraient définir et notifier à la Commission les règles relatives aux sanctions, y compris les amendes administratives, et veiller à ce qu'elles soient correctement et efficacement mises en œuvre à la date d'application du présent règlement. Par conséquent, les dispositions relatives aux sanctions devraient s'appliquer à compter du ... [*douze mois à compter de la date d'entrée en vigueur du présent règlement*].

(180) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphes 1 et 2, du règlement (UE) 2018/1725 et ont rendu leur avis conjoint le 18 juin 2021,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

Chapitre I

Dispositions générales

Article premier

Objet

1. L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, notamment la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation.
2. Le présent règlement établit:
 - a) des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation de systèmes d'IA dans l'Union;
 - b) l'interdiction de certaines pratiques en matière d'IA;
 - c) des exigences spécifiques applicables aux systèmes d'IA à haut risque et des obligations imposées aux opérateurs de ces systèmes;
 - d) des règles harmonisées en matière de transparence applicables à certains systèmes d'IA;
 - e) des règles harmonisées pour la mise sur le marché de modèles d'IA à usage général;

- f) des règles relatives au suivi du marché, à la surveillance du marché, à la gouvernance et à l'application des règles;
- g) des mesures visant à soutenir l'innovation, en mettant particulièrement l'accent sur les PME, y compris les jeunes pousses.

Article 2

Champ d'application

1. Le présent règlement s'applique:

- a) aux fournisseurs établis ou situés dans l'Union ou dans un pays tiers qui mettent sur le marché ou mettent en service des systèmes d'IA ou qui mettent sur le marché des modèles d'IA à usage général dans l'Union;
- b) aux déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans l'Union;
- c) aux fournisseurs et aux déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans un pays tiers, lorsque les sorties produites par le système d'IA sont utilisées dans l'Union;
- d) aux importateurs et aux distributeurs de systèmes d'IA;
- e) aux fabricants de produits qui mettent sur le marché ou mettent en service un système d'IA en même temps que leur produit et sous leur propre nom ou leur propre marque;
- f) aux mandataires des fournisseurs qui ne sont pas établis dans l'Union;
- g) aux personnes concernées qui sont situées dans l'Union.

2. En ce qui concerne les systèmes d'IA classés à haut risque conformément à l'article 6, paragraphe 1, liés aux produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, seuls l'article 6, paragraphe 1, les articles 102 à 109 et l'article 112 s'appliquent. L'article 57 ne s'applique que dans la mesure où les exigences applicables aux systèmes d'IA à haut risque au titre du présent règlement ont été intégrées dans ladite législation d'harmonisation de l'Union.
3. Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en matière de sécurité nationale, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches liées à ces compétences.

Le présent règlement ne s'applique pas aux systèmes d'IA si et dans la mesure où ils sont mis sur le marché, mis en service ou utilisés avec ou sans modifications exclusivement à des fins militaires, de défense ou de sécurité nationale, quel que soit le type d'entité exerçant ces activités.

Le présent règlement ne s'applique pas aux systèmes d'IA qui ne sont pas mis sur le marché ou mis en service dans l'Union, lorsque les sorties sont utilisées dans l'Union exclusivement à des fins militaires, de défense ou de sécurité nationale, quel que soit le type d'entité exerçant ces activités.

4. Le présent règlement ne s'applique ni aux autorités publiques d'un pays tiers ni aux organisations internationales relevant du champ d'application du présent règlement en vertu du paragraphe 1, lorsque ces autorités ou organisations utilisent des systèmes d'IA dans le cadre de la coopération internationale ou d'accords internationaux de coopération des services répressifs et judiciaires avec l'Union ou avec un ou plusieurs États membres, à condition que ce pays tiers ou cette organisation internationale fournisse des garanties adéquates en ce qui concerne la protection des droits fondamentaux et des libertés des personnes.
5. Le présent règlement n'affecte pas l'application des dispositions relatives à la responsabilité des prestataires intermédiaires énoncées au chapitre II du règlement (UE) 2022/2065.
6. Le présent règlement ne s'applique pas aux systèmes d'IA ou aux modèles d'IA spécifiquement développés et mis en service uniquement à des fins de recherche et développement scientifiques, ni à leurs sorties.
7. Le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement n'a pas d'incidence sur le règlement (UE) 2016/679 ou le règlement (UE) 2018/1725, ni sur la directive 2002/58/CE ou la directive (UE) 2016/680, sans préjudice de l'article 10, paragraphe 5, et de l'article 59 du présent règlement.
8. Le présent règlement ne s'applique pas aux activités de recherche, d'essai et de développement relatives aux systèmes d'IA ou modèles d'IA avant leur mise sur le marché ou leur mise en service. Ces activités sont menées conformément au droit de l'Union applicable. Les essais en conditions réelles ne sont pas couverts par cette exclusion.

9. Le présent règlement s'entend sans préjudice des règles établies par d'autres actes juridiques de l'Union relatifs à la protection des consommateurs et à la sécurité des produits.
10. Le présent règlement ne s'applique pas aux obligations incombant aux déployeurs qui sont des personnes physiques utilisant des systèmes d'IA dans le cadre d'une activité strictement personnelle à caractère non professionnel.
11. Le présent règlement n'empêche pas l'Union ou les États membres de maintenir ou d'introduire des dispositions législatives, réglementaires ou administratives plus favorables aux travailleurs quant à la protection de leurs droits en ce qui concerne l'utilisation de systèmes d'IA par les employeurs, ou d'encourager ou de permettre l'application de conventions collectives plus favorables aux travailleurs.
12. Le présent règlement ne s'applique pas aux systèmes d'IA publiés dans le cadre de licences libres et ouvertes, sauf s'ils sont mis sur le marché ou mis en service en tant que systèmes d'IA à haut risque ou en tant que systèmes d'IA qui relèvent de l'article 5 ou de l'article 50.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

- 1) "système d'IA", un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels;

- 2) "risque", la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci;
- 3) "fournisseur", une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit;
- 4) "déployeur", une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel;
- 5) "mandataire", une personne physique ou morale située ou établie dans l'Union ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA ou de modèle d'IA à usage général pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement;
- 6) "importateur", une personne physique ou morale située ou établie dans l'Union qui met sur le marché un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers;
- 7) "distributeur", une personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union;
- 8) "opérateur", un fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur;

- 9) "mise sur le marché", la première mise à disposition d'un système d'IA ou d'un modèle d'IA à usage général sur le marché de l'Union;
- 10) "mise à disposition sur le marché", la fourniture d'un système d'IA ou d'un modèle d'IA à usage général destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;
- 11) "mise en service", la fourniture d'un système d'IA en vue d'une première utilisation directement au déployeur ou pour usage propre dans l'Union, conformément à la destination du système d'IA;
- 12) "destination", l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique;
- 13) "mauvaise utilisation raisonnablement prévisible", l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA;
- 14) "composant de sécurité", un composant d'un produit ou d'un système d'IA qui remplit une fonction de sécurité pour ce produit ou ce système d'IA, ou dont la défaillance ou le dysfonctionnement met en danger la santé et la sécurité des personnes ou des biens;
- 15) "notice d'utilisation", les indications communiquées par le fournisseur pour informer le déployeur, en particulier, de la destination et de l'utilisation correcte d'un système d'IA;

- 16) "rappel d'un système d'IA", toute mesure visant à assurer le retour au fournisseur d'un système d'IA mis à la disposition de déployeurs ou à le mettre hors service ou à désactiver son utilisation;
- 17) "retrait d'un système d'IA", toute mesure visant à empêcher qu'un système d'IA se trouvant dans la chaîne d'approvisionnement ne soit mis à disposition sur le marché;
- 18) "performance d'un système d'IA", la capacité d'un système d'IA à remplir sa destination;
- 19) "autorité notifiante", l'autorité nationale chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle;
- 20) "évaluation de la conformité", la procédure permettant de démontrer que les exigences relatives à un système d'IA à haut risque énoncées au chapitre III, section 2, ont été respectées;
- 21) "organisme d'évaluation de la conformité", un organisme en charge des activités d'évaluation de la conformité par un tiers, y compris la mise à l'essai, la certification et l'inspection;
- 22) "organisme notifié", un organisme d'évaluation de la conformité notifié en application du présent règlement et d'autres actes législatifs d'harmonisation de l'Union pertinents;
- 23) "modification substantielle", une modification apportée à un système d'IA après sa mise sur le marché ou sa mise en service, qui n'est pas prévue ou planifiée dans l'évaluation initiale de la conformité réalisée par le fournisseur et qui a pour effet de nuire à la conformité de ce système aux exigences énoncées au chapitre III, section 2, ou qui entraîne une modification de la destination pour laquelle le système d'IA a été évalué;

- 24) "marquage CE", un marquage par lequel le fournisseur indique qu'un système d'IA est conforme aux exigences du chapitre III, section 2, et d'autres actes législatifs d'harmonisation de l'Union applicables qui en prévoient l'apposition;
- 25) "système de surveillance après commercialisation", l'ensemble des activités réalisées par les fournisseurs de systèmes d'IA pour recueillir et analyser les données issues de l'expérience d'utilisation des systèmes d'IA qu'ils mettent sur le marché ou mettent en service de manière à repérer toute nécessité d'appliquer immédiatement une mesure préventive ou corrective;
- 26) "autorité de surveillance du marché", l'autorité nationale assurant la mission et prenant les mesures prévues par le règlement (UE) 2019/1020;
- 27) "norme harmonisée", une norme harmonisée au sens de l'article 2, paragraphe 1, point c), du règlement (UE) n° 1025/2012;
- 28) "spécification commune", un ensemble de spécifications techniques au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012 qui permettent de satisfaire à certaines exigences établies en vertu du présent règlement;
- 29) "données d'entraînement", les données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînaables;
- 30) "données de validation", les données utilisées pour fournir une évaluation du système d'IA entraîné et pour régler ses paramètres non entraînaables ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement;

- 31) "jeu de données de validation", un jeu de données distinct ou une partie du jeu de données d'entraînement, sous la forme d'une division variable ou fixe;
- 32) "données de test", les données utilisées pour fournir une évaluation indépendante du système d'IA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service;
- 33) "données d'entrée", les données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit une sortie;
- 34) "données biométriques", les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques;
- 35) "identification biométrique", la reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données;
- 36) "vérification biométrique", la vérification "un à un" automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données biométriques à des données biométriques précédemment fournies;
- 37) "catégories particulières de données à caractère personnel", les catégories de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679, à l'article 10 de la directive (UE) 2016/680 et à l'article 10, paragraphe 1, du règlement (UE) 2018/1725;

- 38) "données opérationnelles sensibles", les données opérationnelles relatives à des activités de prévention et de détection des infractions pénales, ainsi que d'enquête ou de poursuites en la matière, dont la divulgation pourrait compromettre l'intégrité des procédures pénales;
- 39) "système de reconnaissance des émotions", un système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques;
- 40) "système de catégorisation biométrique", un système d'IA destiné à affecter des personnes physiques à des catégories spécifiques sur la base de leurs données biométriques, à moins que cela ne soit accessoire à un autre service commercial et strictement nécessaire pour des raisons techniques objectives;
- 41) "système d'identification biométrique à distance", un système d'IA destiné à identifier des personnes physiques sans leur participation active, généralement à distance, en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données;
- 42) "système d'identification biométrique à distance en temps réel", un système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel important et qui comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles;
- 43) "système d'identification biométrique à distance a posteriori", un système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance en temps réel;

- 44) "espace accessible au public", tout espace physique de propriété publique ou privée, accessible à un nombre indéterminé de personnes physiques, indépendamment de l'existence de conditions d'accès à cet espace qui puissent s'appliquer, et indépendamment d'éventuelles restrictions de capacité;
- 45) "autorités répressives",
- a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou
 - b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;
- 46) "activités répressives", des activités menées par les autorités répressives ou pour leur compte pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;
- 47) "Bureau de l'IA", la fonction de la Commission consistant à contribuer à la mise en œuvre, au suivi et à la surveillance des systèmes d'IA et de modèles d'IA à usage général et de la gouvernance de l'IA, établi par la décision de la Commission du 24 janvier 2024; les références faites au Bureau de l'IA dans le présent règlement s'entendent comme faites à la Commission;

- 48) "autorité nationale compétente", une autorité notifiante ou une autorité de surveillance du marché; en ce qui concerne les systèmes d'IA mis en service ou utilisés par les institutions, organes ou organismes de l'Union, les références aux autorités nationales compétentes ou aux autorités de surveillance du marché dans le présent règlement s'entendent comme une référence au Contrôleur européen de la protection des données;
- 49) "incident grave", un incident ou dysfonctionnement d'un système d'IA entraînant directement ou indirectement:
- a) le décès d'une personne ou une atteinte grave à la santé d'une personne;
 - b) une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques;
 - c) la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux;
 - d) un dommage grave à des biens ou à l'environnement;
- 50) "données à caractère personnel", les données à caractère personnel définies à l'article 4, point 1), du règlement (UE) 2016/679;
- 51) "données à caractère non personnel", les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;
- 52) "profilage", le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;

- 53) "plan d'essais en conditions réelles", un document décrivant les objectifs, la méthode, la population et le champ d'application géographique et la portée dans le temps, le suivi, l'organisation et la conduite des essais en conditions réelles;
- 54) "plan du bac à sable", un document adopté conjointement entre le fournisseur participant et l'autorité compétente, qui décrit les objectifs, les conditions, les délais, la méthodologie et les exigences applicables aux activités réalisées au sein du bac à sable;
- 55) "bac à sable réglementaire de l'IA", un cadre contrôlé mis en place par une autorité compétente qui offre aux fournisseurs ou fournisseurs potentiels de systèmes d'IA la possibilité de développer, d'entraîner, de valider et de tester, lorsqu'il y a lieu en conditions réelles, un système d'IA innovant, selon un plan du bac à sable pour une durée limitée sous surveillance réglementaire;
- 56) "maîtrise de l'IA", les compétences, les connaissances et la compréhension qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le contexte du présent règlement, de procéder à un déploiement des systèmes d'IA en toute connaissance de cause, ainsi que de prendre conscience des possibilités et des risques que comporte l'IA, ainsi que des préjudices potentiels qu'elle peut causer;
- 57) "essais en conditions réelles", les essais temporaires d'un système d'IA aux fins de sa destination en conditions réelles en dehors d'un laboratoire ou d'un environnement simulé d'une autre manière, visant à recueillir des données fiables et solides et à évaluer et vérifier la conformité du système d'IA aux exigences du présent règlement; les essais en conditions réelles ne remplissent pas les conditions pour constituer une mise sur le marché ni une mise en service du système d'IA au sens du présent règlement, pour autant que toutes les conditions prévues à l'article 57 ou à l'article 60 soient remplies;

- 58) "participant", aux fins des essais en conditions réelles, une personne physique qui participe à des essais en conditions réelles;
- 59) "consentement éclairé", l'expression libre, spécifique, univoque et volontaire, par un participant, de sa volonté de participer à un essai en conditions réelles particulier, après avoir été informé de tous les éléments de l'essai qui lui permettent de prendre sa décision concernant sa participation;
- 60) "hypertrucage", une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques;
- 61) "infraction de grande ampleur", tout acte ou toute omission contraire au droit de l'Union en matière de protection des intérêts des personnes, qui:
- a) a porté ou est susceptible de porter atteinte aux intérêts collectifs des personnes résidant dans au moins deux États membres autres que celui:
 - i) où l'acte ou l'omission en question a son origine ou a eu lieu;
 - ii) où le fournisseur concerné ou, le cas échéant, son mandataire, est situé ou établi; ou
 - iii) où le déployeur est établi, lorsque l'infraction est commise par le déployeur;

- b) a porté, porte ou est susceptible de porter atteinte aux intérêts collectifs des personnes, qui présente des caractéristiques communes, notamment la même pratique illégale ou la violation du même intérêt, et qui se produit simultanément, commise par le même opérateur, dans au moins trois États membres;
- 62) "infrastructure critique", une infrastructure critique au sens de l'article 2, point 4), de la directive (UE) 2022/2557;
- 63) "modèle d'IA à usage général", un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché;
- 64) "capacités à fort impact", des capacités égales ou supérieures aux capacités enregistrées dans les modèles d'IA à usage général les plus avancés;
- 65) "risque systémique", un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur;

- 66) "système d'IA à usage général", un système d'IA qui est fondé sur un modèle d'IA à usage général et qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA;
- 67) "opération en virgule flottante", toute opération ou assignation mathématique impliquant des nombres en virgule flottante, qui constituent un sous-ensemble des nombres réels généralement représentés sur un ordinateur par un entier de précision fixe suivi d'un exposant entier d'une base fixe;
- 68) "fournisseur en aval", un fournisseur d'un système d'IA, y compris d'un système d'IA à usage général, qui intègre un modèle d'IA, que le modèle d'IA soit fourni par lui-même ou non, et verticalement intégré ou fourni par une autre entité sur la base de relations contractuelles.

Article 4

Maîtrise de l'IA

Les fournisseurs et les déployeurs de systèmes d'IA prennent des mesures pour garantir, dans toute la mesure du possible, un niveau suffisant de maîtrise de l'IA pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte, en prenant en considération leurs connaissances techniques, leur expérience, leur éducation et leur formation, ainsi que le contexte dans lequel les systèmes d'IA sont destinés à être utilisés, et en tenant compte des personnes ou des groupes de personnes à l'égard desquels les systèmes d'IA sont destinés à être utilisés.

Chapitre II

Pratiques interdites en matière d'IA

Article 5

Pratiques interdites en matière d'IA

1. Les pratiques en matière d'IA suivantes sont interdites:
 - a) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales, au-dessous du seuil de conscience d'une personne, ou à des techniques délibérément manipulatrices ou trompeuses, avec pour objectif ou effet d'altérer substantiellement le comportement d'une personne ou d'un groupe de personnes en portant considérablement atteinte à leur capacité à prendre une décision éclairée, amenant ainsi la personne à prendre une décision qu'elle n'aurait pas prise autrement, d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne, à une autre personne ou à un groupe de personnes;
 - b) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite les éventuelles vulnérabilités dues à l'âge, au handicap ou à la situation sociale ou économique spécifique d'une personne physique ou d'un groupe de personnes donné avec pour objectif ou effet d'altérer substantiellement le comportement de cette personne ou d'un membre de ce groupe d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à un tiers;

- c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA pour l'évaluation ou la classification de personnes physiques ou de groupes de personnes au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites, la note sociale conduisant à l'une ou l'autre des situations suivantes, ou aux deux:
 - i) le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes de personnes dans des contextes sociaux dissociés du contexte dans lequel les données ont été générées ou collectées à l'origine;
 - ii) le traitement préjudiciable ou défavorable de certaines personnes ou de groupes de personnes, qui est injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci;
- d) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation d'un système d'IA pour mener des évaluations des risques des personnes physiques visant à évaluer ou à prédire le risque qu'une personne physique commette une infraction pénale, uniquement sur la base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité ou caractéristiques; cette interdiction ne s'applique pas aux systèmes d'IA utilisés pour étayer l'évaluation humaine de l'implication d'une personne dans une activité criminelle, qui est déjà fondée sur des faits objectifs et vérifiables, directement liés à une activité criminelle;
- e) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance;

- f) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement, sauf lorsque l'utilisation du système d'IA est destinée à être mise en place ou mise sur le marché pour des raisons médicales ou de sécurité;
- g) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes de catégorisation biométrique qui catégorisent individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle; cette interdiction ne couvre pas l'étiquetage ou le filtrage d'ensembles de données biométriques acquis légalement, tels que des images, fondés sur des données biométriques ou la catégorisation de données biométriques dans le domaine répressif;
- h) l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs suivants:
 - i) la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues;
 - ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste;

- iii) la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II et punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans.

Le premier alinéa, point h), est sans préjudice de l'article 9 du règlement (UE) 2016/679 pour le traitement des données biométriques à des fins autres que répressives.

- 2. L'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), n'est déployée aux fins énoncées audit point, que pour confirmer l'identité de la personne spécifiquement ciblée et tient compte des éléments suivants:
 - a) la nature de la situation donnant lieu à un éventuel recours au système, en particulier la gravité, la probabilité et l'ampleur du préjudice qui serait causé si le système n'était pas utilisé;
 - b) les conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences.

En outre, l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), du présent article respecte les garanties et conditions nécessaires et proportionnées en ce qui concerne cette utilisation, conformément au droit national qui l'autorise, notamment eu égard aux limitations temporelles, géographiques et relatives aux personnes. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public n'est autorisée que si l'autorité répressive a réalisé une analyse d'impact sur les droits fondamentaux conformément à l'article 27 et a enregistré le système dans la base de données de l'UE prévue par l'article 49. Toutefois, dans des cas d'urgence dûment justifiés, il est possible de commencer à utiliser ces systèmes sans enregistrement dans la base de données de l'UE, à condition que cet enregistrement soit effectué sans retard injustifié.

3. Aux fins du paragraphe 1, premier alinéa, point h), et du paragraphe 2, chaque utilisation à des fins répressives d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public est subordonnée à une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante dont la décision est contraignante de l'État membre dans lequel cette utilisation doit avoir lieu, délivrée sur demande motivée et conformément aux règles détaillées du droit national visées au paragraphe 5. Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser ce système sans autorisation à condition que cette autorisation soit demandée sans retard injustifié, au plus tard dans les 24 heures. Si cette autorisation est rejetée, il est mis fin à l'utilisation avec effet immédiat, et toutes les données, ainsi que les résultats et sorties de cette utilisation, sont immédiatement mis au rebut et supprimés.

L'autorité judiciaire compétente ou une autorité administrative indépendante dont la décision est contraignante n'accorde l'autorisation que si elle estime, sur la base d'éléments objectifs ou d'indications claires qui lui sont présentés, que l'utilisation du système d'identification biométrique à distance en temps réel concerné est nécessaire et proportionnée à la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), tels qu'indiqués dans la demande et, en particulier, que cette utilisation reste limitée au strict nécessaire dans le temps et du point de vue de la portée géographique et personnelle. Lorsqu'elle statue sur la demande, cette autorité tient compte des éléments visés au paragraphe 2. Aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne peut être prise sur la seule base de la sortie du système d'identification biométrique à distance "en temps réel".

4. Sans préjudice du paragraphe 3, toute utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives est notifiée à l'autorité de surveillance du marché concernée et à l'autorité nationale chargée de la protection des données, conformément aux règles nationales visées au paragraphe 5. Cette notification contient, au minimum, les informations visées au paragraphe 6 et n'inclut pas de données opérationnelles sensibles.

5. Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, dans les limites et les conditions énumérées au paragraphe 1, premier alinéa, point h), et aux paragraphes 2 et 3. Les États membres concernés établissent dans leur droit national les règles détaillées nécessaires à la demande, à la délivrance et à l'exercice des autorisations visées au paragraphe 3, ainsi qu'à la surveillance et à l'établissement de rapports y afférents. Ces règles précisent également pour quels objectifs énumérés au paragraphe 1, premier alinéa, point h), et notamment pour quelles infractions pénales visées au point h) iii), les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives. Les États membres notifient ces règles à la Commission au plus tard 30 jours après leur adoption. Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance.
6. Les autorités nationales de surveillance du marché et les autorités nationales chargées de la protection des données des États membres qui ont été notifiées de l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, conformément au paragraphe 4, soumettent à la Commission des rapports annuels sur cette utilisation. À cette fin, la Commission fournit aux États membres et aux autorités nationales en matière de surveillance du marché et de protection des données un modèle comprenant des informations sur le nombre de décisions prises par les autorités judiciaires compétentes ou par une autorité administrative indépendante dont la décision est contraignante en ce qui concerne les demandes d'autorisation conformément au paragraphe 3, ainsi que sur leur résultat.

7. La Commission publie des rapports annuels sur l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, fondés sur des données agrégées dans les États membres sur la base des rapports annuels visés au paragraphe 6. Ces rapports annuels n'incluent pas de données opérationnelles sensibles sur les activités répressives connexes.
8. Le présent article ne porte pas atteinte aux interdictions qui s'appliquent lorsqu'une pratique en matière d'IA enfreint d'autres dispositions du droit de l'Union.

Chapitre III

Systèmes d'IA à haut risque

SECTION 1

CLASSIFICATION DE SYSTEMES D'IA COMME SYSTEMES A HAUT RISQUE

Article 6

Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque

1. Un système d'IA mis sur le marché ou mis en service, qu'il soit ou non indépendant des produits visés aux points a) et b), est considéré comme étant à haut risque lorsque les deux conditions suivantes sont remplies:
 - a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou le système d'IA constitue lui-même un tel produit;

- b) le produit dont le composant de sécurité visé au point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément à la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.
- 2. Outre les systèmes d'IA à haut risque visés au paragraphe 1, les systèmes d'IA visés à l'annexe III sont considérés comme étant à haut risque.
- 3. Par dérogation au paragraphe 2, un système d'IA visé à l'annexe III n'est pas considéré comme étant à haut risque lorsqu'il ne présente pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, y compris en n'ayant pas d'incidence significative sur le résultat de la prise de décision.

Le premier alinéa s'applique lorsqu'une des conditions suivantes est remplie:

- a) le système d'IA est destiné à accomplir un tâche procédurale étroite;
- b) le système d'IA est destiné à améliorer le résultat d'une activité humaine préalablement réalisée;
- c) le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures et n'est pas destiné à se substituer à l'évaluation humaine préalablement réalisée, ni à influencer celle-ci, sans examen humain approprié; ou
- d) le système d'IA est destiné à exécuter une tâche préparatoire en vue d'une évaluation pertinente aux fins des cas d'utilisation visés à l'annexe III.

Nonobstant le premier alinéa, un système d'IA visé à l'annexe III est toujours considéré comme étant à haut risque lorsqu'il effectue un profilage de personnes physiques.

4. Un fournisseur qui considère qu'un système d'IA visé à l'annexe III n'est pas à haut risque documente son évaluation avant que ce système ne soit mis sur le marché ou mis en service. Ce fournisseur est soumis à l'obligation d'enregistrement visée à l'article 49, paragraphe 2. À la demande des autorités nationales compétentes, le fournisseur fournit la documentation de l'évaluation.
5. Après consultation du Comité européen de l'intelligence artificielle (ci-après dénommé "Comité IA"), et au plus tard le ... [18 mois à compter de la date d'entrée en vigueur du présent règlement], la Commission fournit des lignes directrices précisant la mise en œuvre pratique du présent article, conformément à l'article 96, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.
6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier le paragraphe 3, deuxième alinéa, du présent article en ajoutant de nouvelles conditions à celles qui y sont énoncées, ou en les modifiant, lorsqu'il existe des preuves concrètes et fiables de l'existence de systèmes d'IA qui relèvent du champ d'application de l'annexe III, mais qui ne présentent pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques.

7. La Commission adopte des actes délégués conformément à l'article 97 afin de modifier le paragraphe 3, deuxième alinéa, du présent article en supprimant l'une des conditions qui y est établie, lorsqu'il existe des preuves concrètes et fiables attestant que cela est nécessaire pour maintenir le niveau de protection de la santé, de la sécurité et des droits fondamentaux prévu par le présent règlement.
8. Toute modification des conditions établies au paragraphe 3, deuxième alinéa, adoptée conformément aux paragraphes 6 et 7 du présent article ne diminue pas le niveau global de protection de la santé, de la sécurité et des droits fondamentaux prévu par le présent règlement et veille à la cohérence avec les actes délégués adoptés conformément à l'article 7, paragraphe 1, et tient compte des évolutions du marché et des technologies.

Article 7

Modifications de l'annexe III

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe III en y ajoutant des cas d'utilisation de systèmes d'IA à haut risque, ou en les modifiant, lorsque les deux conditions suivantes sont remplies:
 - a) les systèmes d'IA sont destinés à être utilisés dans l'un des domaines énumérés à l'annexe III;
 - b) les systèmes d'IA présentent un risque de préjudice pour la santé et la sécurité, ou un risque d'incidence négative sur les droits fondamentaux, et ce risque est équivalent ou supérieur au risque de préjudice ou d'incidence négative que présentent les systèmes d'IA à haut risque déjà visés à l'annexe III.

2. Lorsqu'elle évalue les conditions visées au paragraphe 1, point b), la Commission tient compte des critères suivants:
- a) la destination du système d'IA;
 - b) la mesure dans laquelle un système d'IA a été utilisé ou est susceptible de l'être;
 - c) la nature et la quantité des données traitées et utilisées par le système d'IA, en particulier le traitement ou l'absence de traitement des catégories particulières de données à caractère personnel;
 - d) la mesure dans laquelle le système d'IA agit de manière autonome et la mesure dans laquelle l'homme peut intervenir pour annuler une décision ou des recommandations susceptibles de causer un préjudice potentiel;
 - e) la mesure dans laquelle l'utilisation d'un système d'IA a déjà causé un préjudice à la santé et à la sécurité, a eu une incidence négative sur les droits fondamentaux ou a suscité de graves préoccupations quant à la probabilité de ce préjudice ou de cette incidence négative, tel que cela ressort, par exemple, des rapports ou allégations documentées soumis aux autorités nationales compétentes ou d'autres rapports, le cas échéant;
 - f) l'ampleur potentielle d'un tel préjudice ou d'une telle incidence négative, notamment en ce qui concerne son intensité et sa capacité d'affecter plusieurs personnes ou d'affecter un groupe particulier de personnes de manière disproportionnée;
 - g) la mesure dans laquelle les personnes ayant potentiellement subi un préjudice ou une incidence négative dépendent des résultats obtenus au moyen d'un système d'IA, notamment parce qu'il n'est pas raisonnablement possible, pour des raisons pratiques ou juridiques, de s'affranchir de ces résultats;

- h) la mesure dans laquelle il existe un déséquilibre de pouvoir, ou les personnes ayant potentiellement subi un préjudice ou une incidence négative se trouvent dans une situation vulnérable par rapport au déployeur d'un système d'IA, notamment en raison du statut, de l'autorité, de connaissances, de circonstances économiques ou sociales ou de l'âge;
- i) la mesure dans laquelle les résultats obtenus en utilisant un système d'IA sont facilement corrigibles ou réversibles, compte tenu des solutions techniques disponibles pour les corriger ou les inverser, les résultats qui ont une incidence négative sur la santé, la sécurité ou les droits fondamentaux ne devant pas être considérés comme facilement corrigibles ou réversibles;
- j) la probabilité que le déploiement du système d'IA présente des avantages pour certaines personnes, certains groupes de personnes ou la société dans son ensemble et la portée de ces avantages, y compris les améliorations éventuelles quant à la sécurité des produits;
- k) la mesure dans laquelle le droit existant de l'Union prévoit:
 - i) des mesures de réparation efficaces en ce qui concerne les risques posés par un système d'IA, à l'exclusion des réclamations en dommages-intérêts;
 - ii) des mesures efficaces destinées à prévenir ou à réduire substantiellement ces risques.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier la liste figurant à l'annexe III en supprimant des systèmes d'IA à haut risque lorsque les deux conditions suivantes sont remplies:
- a) le système d'IA à haut risque concerné ne présente plus de risques substantiels pour les droits fondamentaux, la santé ou la sécurité, compte tenu des critères énumérés au paragraphe 2;
 - b) la suppression ne diminue pas le niveau global de protection de la santé, de la sécurité et des droits fondamentaux en vertu du droit de l'Union.

SECTION 2

EXIGENCES APPLICABLES AUX SYSTEMES D'IA A HAUT RISQUE

Article 8

Respect des exigences

1. Les systèmes d'IA à haut risque respectent les exigences énoncées dans la présente section, en tenant compte de leur destination ainsi que de l'état de la technique généralement reconnu en matière d'IA et de technologies liées à l'IA. Pour garantir le respect de ces exigences, il est tenu compte du système de gestion des risques prévu à l'article 9.

2. Lorsqu'un produit contient un système d'IA auquel s'appliquent les exigences du présent règlement ainsi que les exigences de la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, les fournisseurs sont chargés de veiller à ce que leur produit soit pleinement conforme à toutes les exigences en vertu de la législation d'harmonisation de l'Union applicable. Pour garantir que les systèmes d'IA à haut risque visés au paragraphe 1 sont conformes aux exigences énoncées dans la présente section, et afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les processus d'essai et de déclaration nécessaires, les informations et la documentation qu'ils fournissent concernant leur produit dans la documentation et les procédures qui existent déjà et qui sont requises en vertu de la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I.

Article 9

Système de gestion des risques

1. Un système de gestion des risques est établi, mis en œuvre, documenté et tenu à jour en ce qui concerne les systèmes d'IA à haut risque.
2. Ce système de gestion des risques s'entend comme étant un processus itératif continu qui est planifié et se déroule sur l'ensemble du cycle de vie d'un système d'IA à haut risque et qui doit périodiquement faire l'objet d'un examen et d'une mise à jour méthodiques. Il comprend les étapes suivantes:
 - a) l'identification et l'analyse des risques connus et raisonnablement prévisibles que le système d'IA à haut risque peut poser pour la santé, la sécurité ou les droits fondamentaux lorsque le système d'IA à haut risque est utilisé conformément à sa destination;

- b) l'estimation et l'évaluation des risques susceptibles d'apparaître lorsque le système d'IA à haut risque est utilisé conformément à sa destination et dans des conditions de mauvaise utilisation raisonnablement prévisible;
 - c) l'évaluation d'autres risques susceptibles d'apparaître, sur la base de l'analyse des données recueillies au moyen du système de surveillance après commercialisation visé à l'article 72;
 - d) l'adoption de mesures appropriées et ciblées de gestion des risques, conçues pour répondre aux risques identifiés en vertu du point a).
3. Les risques visés au présent article ne concernent que ceux qui peuvent être raisonnablement atténués ou éliminés dans le cadre du développement ou de la conception du système d'IA à haut risque, ou par la fourniture d'informations techniques appropriées.
4. Les mesures de gestion des risques visées au paragraphe 2, point d), tiennent dûment compte des effets et de l'interaction possibles résultant de l'application combinée des exigences énoncées dans la présente section, en vue de prévenir les risques plus efficacement tout en parvenant à un bon équilibre dans le cadre de la mise en œuvre des mesures visant à répondre à ces exigences.
5. Les mesures de gestion des risques visées au paragraphe 2, point d), sont telles que le risque résiduel pertinent associé à chaque danger ainsi que le risque résiduel global lié aux systèmes d'IA à haut risque sont jugés acceptables.

Pour déterminer les mesures de gestion des risques les plus adaptées, il convient de veiller à:

- a) éliminer ou réduire les risques identifiés et évalués conformément au paragraphe 2 autant que la technologie le permet grâce à une conception et à un développement appropriés du système d'IA à haut risque;
- b) mettre en œuvre, le cas échéant, des mesures adéquates d'atténuation et de contrôle répondant aux risques impossibles à éliminer;
- c) fournir aux déployeurs les informations requises conformément à l'article 13 et, éventuellement, une formation.

En vue de l'élimination ou de la réduction des risques liés à l'utilisation du système d'IA à haut risque, il est dûment tenu compte des connaissances techniques, de l'expérience, de l'éducation et de la formation pouvant être attendues du déployeur, ainsi que du contexte prévisible dans lequel le système est destiné à être utilisé.

- 6. Les systèmes d'IA à haut risque sont soumis à des essais afin de déterminer les mesures de gestion des risques les plus appropriées et les plus ciblées. Les essais garantissent que les systèmes d'IA à haut risque fonctionnent de manière conforme à leur destination et qu'ils sont conformes aux exigences énoncées dans la présente section.
- 7. Les procédures d'essai peuvent comprendre des essais en conditions réelles conformément à l'article 60.

8. Les tests des systèmes d'IA à haut risque sont effectués, selon les besoins, à tout moment pendant le processus de développement et, en tout état de cause, avant leur mise sur le marché ou leur mise en service. Les tests sont effectués sur la base d'indicateurs et de seuils probabilistes préalablement définis, qui sont adaptés à la destination du système d'IA à haut risque.
9. Lors de la mise en œuvre du système de gestion des risques prévu aux paragraphes 1 à 7, les fournisseurs prennent en considération la probabilité que, compte tenu de sa destination, le système d'IA à haut risque puisse avoir une incidence négative sur des personnes âgées de moins de 18 ans et, le cas échéant, sur d'autres groupes vulnérables.
10. En ce qui concerne les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des exigences concernant les processus internes de gestion des risques en vertu d'autres dispositions pertinentes du droit de l'Union, les aspects présentés aux paragraphes 1 à 9 peuvent faire partie des procédures de gestion des risques établies conformément à ladite législation, ou être combinées à celles-ci.

Article 10

Données et gouvernance des données

1. Les systèmes d'IA à haut risque faisant appel à des techniques qui impliquent l'entraînement de modèles d'IA au moyen de données sont développés sur la base de jeux de données d'entraînement, de validation et de test qui satisfont aux critères de qualité visés aux paragraphes 2 à 5 chaque fois que ces jeux de données sont utilisés.

2. Les jeux de données d'entraînement, de validation et de test sont soumis à des pratiques en matière de gouvernance et de gestion des données appropriées à la destination du systèmes d'IA à haut risque. Ces pratiques concernent en particulier:
- a) les choix de conception pertinents;
 - b) les processus de collecte de données et l'origine des données, ainsi que, dans le cas des données à caractère personnel, la finalité initiale de la collecte de données;
 - c) les opérations de traitement pertinentes pour la préparation des données, telles que l'annotation, l'étiquetage, le nettoyage, la mise à jour, l'enrichissement et l'agrégation;
 - d) la formulation d'hypothèses, notamment en ce qui concerne les informations que les données sont censées mesurer et représenter;
 - e) une évaluation de la disponibilité, de la quantité et de l'adéquation des jeux de données nécessaires;
 - f) un examen permettant de repérer d'éventuels biais qui sont susceptibles de porter atteinte à la santé et à la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de se traduire par une discrimination interdite par le droit de l'Union, en particulier lorsque les données de sortie influencent les entrées pour les opérations futures;
 - g) les mesures appropriées visant à détecter, prévenir et atténuer les éventuels biais repérés conformément au point f);
 - h) la détection de lacunes ou déficiences pertinentes dans les données qui empêchent l'application du présent règlement, et la manière dont ces lacunes ou déficiences peuvent être comblées.

3. Les jeux de données d'entraînement, de validation et de test sont pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination. Ils possèdent les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le système d'IA à haut risque est destiné à être utilisé. Ces caractéristiques des jeux de données peuvent être remplies au niveau des jeux de données pris individuellement ou d'une combinaison de ceux-ci.
4. Les jeux de données tiennent compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé.
5. Dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, conformément au paragraphe 2, points f) et g), du présent article, les fournisseurs de ces systèmes peuvent exceptionnellement traiter des catégories particulières de données à caractère personnel, sous réserve de garanties appropriées pour les droits et libertés fondamentaux des personnes physiques. Outre les dispositions des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680, toutes les conditions suivantes doivent être réunies pour que ce traitement puisse avoir lieu:
 - a) la détection et la correction des biais ne peuvent être satisfaites de manière efficace en traitant d'autres données, y compris des données synthétiques ou anonymisées;

- b) les catégories particulières de données à caractère personnel sont soumises à des limitations techniques relatives à la réutilisation des données à caractère personnel, ainsi qu'aux mesures les plus avancées en matière de sécurité et de protection de la vie privée, y compris la pseudonymisation;
- c) les catégories particulières de données à caractère personnel font l'objet de mesures visant à garantir que les données à caractère personnel traitées sont sécurisées, protégées et soumises à des garanties appropriées, y compris des contrôles stricts et une documentation de l'accès, afin d'éviter toute mauvaise utilisation et de veiller à ce que seules les personnes autorisées ayant des obligations de confidentialité appropriées aient accès à ces données à caractère personnel;
- d) les catégories particulières de données à caractère personnel ne doivent pas être transmises, transférées ou consultées d'une autre manière par d'autres parties;
- e) les catégories particulières de données à caractère personnel sont supprimées une fois que le biais a été corrigé ou que la période de conservation des données à caractère personnel a expiré, selon celle de ces deux échéances qui arrive en premier;
- f) les registres des activités de traitement visés dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680 comprennent les raisons pour lesquelles le traitement des catégories particulières de données à caractère personnel était strictement nécessaire pour détecter et corriger les biais, ainsi que la raison pour laquelle cet objectif n'a pas pu être atteint par le traitement d'autres données.

6. En ce qui concerne le développement de systèmes d'IA à haut risque qui ne font pas appel à des techniques qui impliquent l'entraînement de modèles d'IA, les paragraphes 2 à 5 s'appliquent uniquement aux jeux de données de test.

Article 11
Documentation technique

1. La documentation technique relative à un système d'IA à haut risque est établie avant que ce système ne soit mis sur le marché ou mis en service et est tenue à jour.

La documentation technique est établie de manière à démontrer que le système d'IA à haut risque satisfait aux exigences énoncées dans la présente section et à fournir aux autorités nationales compétentes et aux organismes notifiés les informations nécessaires sous une forme claire et intelligible pour évaluer la conformité du système d'IA avec ces exigences. Elle contient, au minimum, les éléments énoncés à l'annexe IV. Les PME, y compris les jeunes pousses, peuvent fournir des éléments de la documentation technique spécifiée à l'annexe IV d'une manière simplifiée. À cette fin, la Commission établit un formulaire de documentation technique simplifié ciblant les besoins des petites entreprises et des microentreprises. Lorsqu'une PME, y compris une jeune pousse, choisit de fournir les informations requises à l'annexe IV de manière simplifiée, elle utilise le formulaire visé au présent paragraphe. Les organismes notifiés acceptent le formulaire aux fins de l'évaluation de la conformité.

2. Lorsqu'un système d'IA à haut risque lié à un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I est mis sur le marché ou mis en service, un seul ensemble de documentation technique est établi, contenant toutes les informations visées au paragraphe 1, ainsi que les informations requises en vertu de ces actes juridiques.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe IV, lorsque cela est nécessaire, afin de garantir que, compte tenu du progrès technique, la documentation technique fournit toutes les informations requises pour évaluer la conformité du système avec les exigences énoncées dans la présente section.

Article 12

Enregistrement

1. Les systèmes d'IA à haut risque permettent, techniquement, l'enregistrement automatique des événements (journaux) tout au long de la durée de vie du système.
2. Afin de garantir un degré de traçabilité du fonctionnement d'un système d'IA qui soit adapté à la destination du système, les fonctionnalités de journalisation permettent l'enregistrement des événements pertinents pour:
 - a) repérer les situations susceptibles d'avoir pour effet que le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, ou d'entraîner une modification substantielle;
 - b) faciliter la surveillance après commercialisation visée à l'article 72; et
 - c) surveiller le fonctionnement du système d'IA à haut risque comme prévu à l'article 26, paragraphe 5.
3. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les fonctionnalités de journalisation fournissent, au minimum:
 - a) l'enregistrement de la période de chaque utilisation du système (date et heure de début et de fin pour chaque utilisation);

- b) la base de données de référence utilisée par le système pour vérifier les données d'entrée;
- c) les données d'entrée pour lesquelles la recherche a abouti à une correspondance;
- d) l'identification des personnes physiques participant à la vérification des résultats, visées à l'article 14, paragraphe 5.

Article 13

Transparence et fourniture d'informations aux déployeurs

1. La conception et le développement des systèmes d'IA à haut risque sont tels que le fonctionnement de ces systèmes est suffisamment transparent pour permettre aux déployeurs d'interpréter les sorties d'un système et de les utiliser de manière appropriée. Un type et un niveau adéquats de transparence sont garantis afin de veiller au respect des obligations pertinentes incombant au fournisseur et au déployeur énoncées à la section 3.
2. Les systèmes d'IA à haut risque sont accompagnés d'une notice d'utilisation dans un format numérique approprié ou autre, contenant des informations concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les déployeurs.
3. La notice d'utilisation contient au moins les informations suivantes:
 - a) l'identité et les coordonnées du fournisseur et, le cas échéant, de son mandataire;

- b) les caractéristiques, les capacités et les limites de performance du système d'IA à haut risque, notamment:
- i) sa destination;
 - ii) le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité visé à l'article 15 qui a servi de référence pour les tests et la validation du système d'IA à haut risque et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité;
 - iii) toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé et la sécurité ou pour les droits fondamentaux visés à l'article 9, paragraphe 2;
 - iv) le cas échéant, les capacités et caractéristiques techniques du système d'IA à haut risque à fournir des informations pertinentes pour expliquer ses sorties;
 - v) le cas échéant, sa performance en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé;
 - vi) le cas échéant, les spécifications relatives aux données d'entrée, ou toute autre information pertinente concernant les jeux de données d'entraînement, de validation et de test utilisés, compte tenu de la destination du système d'IA à haut risque;

- vii) le cas échéant, les informations permettant aux dépoyeurs d'interpréter les sorties du système d'IA à haut risque et de les utiliser de manière appropriée;
- c) les modifications du système d'IA à haut risque et de sa performance qui ont été prédéterminées par le fournisseur au moment de l'évaluation initiale de la conformité, le cas échéant;
- d) les mesures de contrôle humain visées à l'article 14, notamment les mesures techniques mises en place pour faciliter l'interprétation des sorties des systèmes d'IA à haut risque par les dépoyeurs;
- e) les ressources informatiques et matérielles nécessaires, la durée de vie attendue du système d'IA à haut risque et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement de ce système d'IA, notamment en ce qui concerne les mises à jour logicielles;
- f) le cas échéant, une description des mécanismes compris dans le système d'IA à haut risque qui permet aux dépoyeurs de collecter, stocker et interpréter correctement les journaux, conformément à l'article 12.

Article 14

Contrôle humain

1. La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant leur période d'utilisation.

2. Le contrôle humain vise à prévenir ou à réduire au minimum les risques pour la santé, la sécurité ou les droits fondamentaux qui peuvent apparaître lorsqu'un système d'IA à haut risque est utilisé conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, en particulier lorsque de tels risques persistent malgré l'application d'autres exigences énoncées dans la présente section.
3. Les mesures de contrôle sont proportionnées aux risques, au niveau d'autonomie et au contexte d'utilisation du système d'IA à haut risque, et sont assurées au moyen d'un ou des deux types de mesures suivants:
 - a) des mesures identifiées et, lorsque cela est techniquement possible, intégrées par le fournisseur dans le système d'IA à haut risque avant la mise sur le marché ou la mise en service de ce dernier;
 - b) des mesures identifiées par le fournisseur avant la mise sur le marché ou la mise en service du système d'IA à haut risque et qui se prêtent à une mise en œuvre par le déployeur.
4. Aux fins de la mise en œuvre des dispositions des paragraphes 1, 2 et 3, le système d'IA à haut risque est fourni au déployeur de telle manière que les personnes physiques chargées d'effectuer un contrôle humain, dans la mesure où cela est approprié et proportionné, ont la possibilité:
 - a) de comprendre correctement les capacités et les limites pertinentes du système d'IA à haut risque et d'être en mesure de surveiller correctement son fonctionnement, y compris en vue de détecter et de traiter les anomalies, les dysfonctionnements et les performances inattendues;

- b) d'avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux sorties produites par un système d'IA à haut risque (biais d'automatisation), en particulier pour les systèmes d'IA à haut risque utilisés pour fournir des informations ou des recommandations concernant les décisions à prendre par des personnes physiques;
- c) d'interpréter correctement les sorties du système d'IA à haut risque, compte tenu par exemple des outils et méthodes d'interprétation disponibles;
- d) de décider, dans une situation particulière, de ne pas utiliser le système d'IA à haut risque ou d'ignorer, remplacer ou inverser la sortie du système d'IA à haut risque;
- e) d'intervenir dans le fonctionnement du système d'IA à haut risque ou d'interrompre le système au moyen d'un bouton d'arrêt ou d'une procédure similaire permettant au système de s'arrêter de manière sécurisée.

5. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les mesures prévues au paragraphe 3 du présent article sont de nature à garantir que, en outre, aucune mesure ou décision n'est prise par le déployeur sur la base de l'identification résultant du système sans vérification et confirmation distinctes de cette identification par au moins deux personnes physiques disposant des compétences, de la formation et de l'autorité nécessaires.

L'exigence d'une vérification distincte par au moins deux personnes physiques ne s'applique pas aux systèmes d'IA à haut risque utilisés à des fins répressives ou dans les domaines de la migration, des contrôles aux frontières ou de l'asile, lorsque le droit de l'Union ou le droit national considère que l'application de cette exigence est disproportionnée.

Article 15

Exactitude, robustesse et cybersécurité

1. La conception et le développement des systèmes d'IA à haut risque sont tels qu'ils leur permettent d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de façon constante à cet égard tout au long de leur cycle de vie.
2. Pour examiner les aspects techniques de la manière de mesurer les niveaux appropriés d'exactitude et de robustesse visés au paragraphe 1 et tout autre indicateur de performance pertinent, la Commission, en coopération avec les parties prenantes et organisations concernées, telles que les autorités de métrologie et d'étalonnage des performances, encourage, le cas échéant, l'élaboration de critères de référence et de méthodes de mesure.
3. Les niveaux d'exactitude et les indicateurs de l'exactitude des systèmes d'IA à haut risque sont indiqués dans la notice d'utilisation jointe.
4. Les systèmes d'IA à haut risque font preuve d'autant de résilience que possible en cas d'erreurs, de défaillances ou d'incohérences pouvant survenir au sein des systèmes eux-mêmes ou de l'environnement dans lequel ils fonctionnent, notamment en raison de leur interaction avec des personnes physiques ou d'autres systèmes. Des mesures techniques et organisationnelles sont prises à cet égard.

Des solutions techniques redondantes, telles que des plans de sauvegarde ou des mesures de sécurité après défaillance, peuvent permettre de garantir la robustesse des systèmes d'IA à haut risque.

Les systèmes d'IA à haut risque qui continuent leur apprentissage après leur mise sur le marché ou leur mise en service sont développés de manière à éliminer ou à réduire dans la mesure du possible le risque que des sorties éventuellement biaisées n'influencent les entrées pour les opérations futures (boucles de rétroaction) et à veiller à ce que ces boucles de rétroaction fassent l'objet d'un traitement adéquat au moyen de mesures d'atténuation appropriées.

5. Les systèmes d'IA à haut risque résistent aux tentatives de tiers non autorisés visant à modifier leur utilisation, leurs sorties ou leur performance en exploitant les vulnérabilités du système.

Les solutions techniques visant à garantir la cybersécurité des systèmes d'IA à haut risque sont adaptées aux circonstances pertinentes et aux risques.

Les solutions techniques destinées à remédier aux vulnérabilités spécifiques à l'IA comprennent, au besoin, des mesures ayant pour but de prévenir, de détecter, de contrer, de résoudre et de maîtriser les attaques visant à manipuler le jeu de données d'entraînement (empoisonnement des données) ou les composants préentraînés utilisés en entraînement (empoisonnement de modèle), les entrées destinées à induire le modèle d'IA en erreur (exemples contradictoires ou invasion de modèle), les attaques visant la confidentialité ou les défauts du modèle.

SECTION 3

OBLIGATIONS INCOMBANT AUX FOURNISSEURS

ET AUX DEPLOYEURS DE SYSTEMES D'IA A HAUT RISQUE ET A D'AUTRES PARTIES

Article 16

Obligations incombant aux fournisseurs de systèmes d'IA à haut risque

Les fournisseurs de systèmes d'IA à haut risque:

- a) veillent à ce que leurs systèmes d'IA à haut risque soient conformes aux exigences énoncées à la section 2;
- b) indiquent sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur son emballage ou dans la documentation l'accompagnant, selon le cas, leur nom, raison sociale ou marque déposée, l'adresse à laquelle ils peuvent être contactés;
- c) mettent en place un système de gestion de la qualité conforme à l'article 17;
- d) assurent la conservation de la documentation visée à l'article 18;
- e) assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, lorsque ces journaux se trouvent sous leur contrôle, conformément à l'article 19;
- f) veillent à ce que le système d'IA à haut risque soit soumis à la procédure d'évaluation de la conformité applicable visée à l'article 43, avant sa mise sur le marché ou sa mise en service;

- g) élaborent une déclaration UE de conformité conformément à l'article 47;
- h) apposent le marquage CE sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur son emballage ou dans la documentation l'accompagnant, selon le cas, afin d'indiquer la conformité avec le présent règlement, conformément à l'article 48;
- i) respectent les obligations en matière d'enregistrement prévues à l'article 49, paragraphe 1;
- j) prennent les mesures correctives nécessaires et fournissent les informations requises à l'article 20;
- k) à la demande motivée d'une autorité nationale compétente, prouvent la conformité du système d'IA à haut risque avec les exigences énoncées à la section 2;
- l) veillent à ce que le système d'IA à haut risque soit conforme aux exigences en matière d'accessibilité conformément aux directives (UE) 2016/2102 et (UE) 2019/882.

Article 17

Système de gestion de la qualité

1. Les fournisseurs de systèmes d'IA à haut risque mettent en place un système de gestion de la qualité garantissant le respect du présent règlement. Ce système est documenté de manière méthodique et ordonnée sous la forme de politiques, de procédures et d'instructions écrites, et comprend au moins les aspects suivants:
 - a) une stratégie de respect de la réglementation, notamment le respect des procédures d'évaluation de la conformité et des procédures de gestion des modifications apportées aux systèmes d'IA à haut risque;

- b) des techniques, procédures et actions systématiques destinées à la conception des systèmes d'IA à haut risque ainsi qu'au contrôle et à la vérification de cette conception;
- c) des techniques, procédures et actions systématiques destinées au développement des systèmes d'IA à haut risque ainsi qu'au contrôle et à l'assurance de leur qualité;
- d) des procédures d'examen, de test et de validation à exécuter avant, pendant et après le développement du système d'IA à haut risque, ainsi que la fréquence à laquelle elles doivent être réalisées;
- e) des spécifications techniques, notamment des normes, à appliquer et, lorsque les normes harmonisées pertinentes ne sont pas appliquées intégralement, ou ne couvrent pas toutes les exigences pertinentes énoncées à la section 2, les moyens à utiliser pour faire en sorte que le système d'IA à haut risque satisfasse auxdites exigences;
- f) les systèmes et procédures de gestion des données, notamment l'acquisition, la collecte, l'analyse, l'étiquetage, le stockage, la filtration, l'exploration, l'agrégation, la conservation des données et toute autre opération concernant les données qui est effectuée avant la mise sur le marché ou la mise en service de systèmes d'IA à haut risque et aux fins de celles-ci;
- g) le système de gestion des risques prévu à l'article 9;
- h) l'élaboration, la mise en œuvre et le fonctionnement d'un système de surveillance après commercialisation conformément à l'article 72;

- i) les procédures relatives au signalement d'un incident grave conformément à l'article 73;
 - j) la gestion des communications avec les autorités nationales compétentes, les autres autorités compétentes, y compris celles fournissant ou facilitant l'accès aux données, les organismes notifiés, les autres opérateurs, les clients ou d'autres parties intéressées;
 - k) les systèmes et procédures de conservation de tous les documents et informations pertinents;
 - l) la gestion des ressources, y compris les mesures liées à la sécurité d'approvisionnement;
 - m) un cadre de responsabilisation définissant les responsabilités de l'encadrement et des autres membres du personnel en ce qui concerne tous les aspects énumérés dans le présent paragraphe.
2. La mise en œuvre des aspects visés au paragraphe 1 est proportionnée à la taille de l'organisation du fournisseur. Les fournisseurs respectent, en tout état de cause, le degré de rigueur et le niveau de protection requis afin de garantir que leurs systèmes d'IA à haut risque sont conformes au présent règlement.
3. Les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des obligations relatives aux systèmes de gestion de la qualité, ou liées à l'exercice d'une fonction équivalente en vertu de la législation sectorielle pertinente de l'Union peuvent inclure les aspects énumérés au paragraphe 1 dans les systèmes de gestion de la qualité conformément à ladite législation.

4. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, la conformité avec les règles relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues dans la législation pertinente de l'Union sur les services financiers vaut respect de l'obligation de mettre en place un système de gestion de la qualité, à l'exception du paragraphe 1, points g), h) et i) du présent article. À cette fin, toute norme harmonisée visée à l'article 40 est prise en considération.

Article 18

Conservation des documents

1. Pendant une période prenant fin 10 ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, le fournisseur tient à la disposition des autorités nationales compétentes:
- a) la documentation technique visée à l'article 11;
 - b) la documentation concernant le système de gestion de la qualité visé à l'article 17;
 - c) la documentation concernant les modifications approuvées par les organismes notifiés, le cas échéant;
 - d) les décisions et autres documents émis par les organismes notifiés, le cas échéant;
 - e) la déclaration UE de conformité visée à l'article 47.

2. Chaque État membre détermine les conditions dans lesquelles la documentation visée au paragraphe 1 reste à la disposition des autorités nationales compétentes pendant la période indiquée audit paragraphe dans le cas où un fournisseur ou son mandataire établi sur son territoire fait faillite ou met un terme à ses activités avant la fin de cette période.
3. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour la documentation technique dans le cadre de la documentation conservée en vertu de la législation pertinente de l'Union sur les services financiers.

Article 19

Journaux générés automatiquement

1. Les fournisseurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous leur contrôle. Sans préjudice du droit de l'Union ou du droit national applicable, les journaux sont conservés pendant une période adaptée à la destination du système d'IA à haut risque, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.
2. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour les journaux générés automatiquement par leurs systèmes d'IA à haut risque dans le cadre de la documentation conservée en vertu de la législation pertinente sur les services financiers.

Article 20

Mesures corrective et devoir d'information

1. Les fournisseurs de systèmes d'IA à haut risque qui considèrent ou ont des raisons de considérer qu'un système d'IA à haut risque qu'ils ont mis sur le marché ou mis en service n'est pas conforme au présent règlement prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité, le retirer, le désactiver ou le rappeler, selon le cas. Ils informent les distributeurs du système d'IA à haut risque concerné et, le cas échéant, les déployeurs, le mandataire et les importateurs en conséquence.
2. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, et que le fournisseur prend conscience de ce risque, celui-ci recherche immédiatement les causes, en collaboration avec le déployeur à l'origine du signalement, le cas échéant, et informe les autorités de surveillance du marché compétentes pour le système d'IA à haut risque concerné et, le cas échéant, l'organisme notifié qui a délivré un certificat pour ce système d'IA à haut risque, conformément à l'article 44, en précisant en particulier la nature du cas de non-conformité et les éventuelles mesures correctives pertinentes prises.

Article 21

Coopération avec les autorités compétentes

1. À la demande motivée d'une autorité compétente, les fournisseurs de systèmes d'IA à haut risque fournissent à ladite autorité toutes les informations et tous les documents nécessaires pour démontrer la conformité du système d'IA à haut risque avec les exigences énoncées à la section 2, dans une langue aisément compréhensible par l'autorité dans l'une des langues officielles des institutions de l'Union, telle qu'indiquée par l'État membre concerné.
2. À la demande motivée d'une autorité compétente, les fournisseurs accordent également à l'autorité compétente à l'origine de la demande, le cas échéant, l'accès aux journaux générés automatiquement par le système d'IA à haut risque visés à l'article 12, paragraphe 1, dans la mesure où ces journaux sont sous leur contrôle.
3. Les informations obtenues par une autorité compétente en application du présent article sont traitées conformément aux obligations de confidentialité énoncées à l'article 78.

Article 22

Mandataires des fournisseurs de systèmes d'IA à haut risque

1. Avant de mettre leurs systèmes d'IA à haut risque à disposition sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le fournisseur autorise son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.
3. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Il fournit une copie du mandat aux autorités de surveillance du marché à leur demande, dans l'une des langues officielles des institutions de l'Union, indiquée par l'autorité compétente. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter les tâches suivantes:
 - a) vérifier que la déclaration UE de conformité visée à l'article 47 et la documentation technique visée à l'article 11 ont été établies et que le fournisseur a suivi une procédure appropriée d'évaluation de la conformité;
 - b) tenir à la disposition des autorités compétentes et des autorités ou organismes nationaux visés à l'article 74, paragraphe 10, pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les coordonnées du fournisseur ayant désigné le mandataire, une copie de la déclaration UE de conformité visée à l'article 47, la documentation technique et, le cas échéant, le certificat délivré par l'organisme notifié;
 - c) à la demande motivée d'une autorité compétente, communiquer à cette dernière toutes les informations et tous les documents, y compris ceux visés au point b) du présent alinéa, nécessaires pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, et notamment lui donner accès aux journaux générés automatiquement par le système d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous le contrôle du fournisseur;

- d) à la demande motivée des autorités compétentes, coopérer avec elles à toute mesure prise par ces dernières à l'égard du système d'IA à haut risque, en particulier pour réduire et atténuer les risques posés par le système d'IA à haut risque;
- e) le cas échéant, respecter les obligations en matière d'enregistrement visées à l'article 49, paragraphe 1, ou, si l'enregistrement est effectué par le fournisseur lui-même, vérifier que les informations visées à l'annexe VIII, section A, point 3, sont correctes.

Le mandat habilite le mandataire à servir d'interlocuteur, en plus ou à la place du fournisseur, aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.

- 4. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent en vertu du présent règlement. Dans ce cas, il informe immédiatement l'autorité de surveillance du marché concernée et, selon le cas, l'organisme notifié pertinent de la cessation du mandat et des motifs qui la sous-tendent.

Article 23

Obligations des importateurs

- 1. Avant de mettre sur le marché un système d'IA à haut risque, les importateurs s'assurent que le système est conforme au présent règlement en vérifiant que:
 - a) le fournisseur du système d'IA à haut risque a suivi la procédure pertinente d'évaluation de la conformité visée à l'article 43;

- b) le fournisseur a établi la documentation technique conformément à l'article 11 et à l'annexe IV;
 - c) le système porte le marquage CE requis et est accompagné de la déclaration UE de conformité visée à l'article 47 et de la notice d'utilisation;
 - d) le fournisseur a désigné un mandataire conformément à l'article 22, paragraphe 1.
2. Lorsqu'un importateur a des raisons suffisantes de considérer qu'un système d'IA à haut risque n'est pas conforme au présent règlement, ou a été falsifié ou s'accompagne de documents falsifiés, il ne met le système sur le marché qu'après sa mise en conformité. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, l'importateur en informe le fournisseur du système, les mandataires et les autorités de surveillance du marché.
3. Les importateurs indiquent leur nom, raison sociale ou marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés, sur le système d'IA à haut risque et sur son emballage ou dans la documentation l'accompagnant, selon le cas.
4. Les importateurs s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport, le cas échéant, ne compromettent pas sa conformité avec les exigences énoncées à la section 2.

5. Pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les importateurs conservent une copie du certificat délivré par l'organisme notifié, selon le cas, de la notice d'utilisation et de la déclaration UE de conformité visée à l'article 47.
6. À la demande motivée des autorités compétentes concernées, les importateurs communiquent à ces dernières toutes les informations et tous les documents nécessaires, y compris ceux visés au paragraphe 5, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, dans une langue aisément compréhensible par les autorités nationales compétentes. À cette fin, ils veillent également à ce que la documentation technique puisse être mise à la disposition de ces autorités.
7. Les importateurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un système d'IA à haut risque mis sur le marché par les importateurs, en particulier pour réduire et atténuer les risques qu'il présente.

Article 24

Obligations des distributeurs

1. Avant de mettre un système d'IA à haut risque à disposition sur le marché, les distributeurs vérifient qu'il porte le marquage CE requis, qu'il est accompagné d'une copie de la déclaration UE de conformité visée à l'article 47 et de la notice d'utilisation, et que le fournisseur et l'importateur dudit système, selon le cas, ont respecté leurs obligations respectives en vertu de l'article 16, points b) et c), et de l'article 23, paragraphe 3.

2. Lorsqu'un distributeur considère ou a des raisons de considérer, sur la base des informations en sa possession, qu'un système d'IA à haut risque n'est pas conforme aux exigences énoncées à la section 2, il ne met le système à disposition sur le marché qu'après la mise en conformité de celui-ci avec lesdites exigences. De plus, lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, le distributeur en informe le fournisseur ou l'importateur du système, selon le cas.
3. Les distributeurs s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport, le cas échéant, ne compromettent pas sa conformité avec les exigences énoncées à la section 2.
4. Lorsqu'un distributeur considère ou a des raisons de considérer, sur la base des informations en sa possession, qu'un système d'IA à haut risque qu'il a mis à disposition sur le marché n'est pas conforme aux exigences énoncées à la section 2, il prend les mesures correctives nécessaires pour mettre ce système en conformité avec lesdites exigences, le retirer ou le rappeler ou veille à ce que le fournisseur, l'importateur ou tout opérateur concerné, selon le cas, prenne ces mesures correctives. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, le distributeur en informe immédiatement le fournisseur ou l'importateur du système ainsi que les autorités compétentes pour le système d'IA à haut risque concerné et précise, notamment, le cas de non-conformité et les éventuelles mesures correctives prises.

5. À la demande motivée d'une autorité compétente concernée, les distributeurs d'un système d'IA à haut risque communiquent à cette autorité toutes les informations et tous les documents concernant les mesures qu'ils ont prises en vertu des paragraphes 1 à 4, nécessaires pour démontrer la conformité de ce système avec les exigences énoncées à la section 2.
6. Les distributeurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un système d'IA à haut risque mis à disposition sur le marché par les distributeurs, en particulier pour réduire et atténuer les risques qu'il présente.

Article 25

Responsabilités tout au long de la chaîne de valeur de l'IA

1. Tout distributeur, importateur, déployeur ou autre tiers est considéré comme un fournisseur d'un système d'IA à haut risque aux fins du présent règlement et est soumis aux obligations incombant au fournisseur au titre de l'article 16 dans toutes les circonstances suivantes:
 - a) il commercialise sous son propre nom ou sa propre marque un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles prévoyant une autre répartition des obligations;
 - b) il apporte une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service de telle manière qu'il reste un système d'IA à haut risque en application de l'article 6;

c) il modifie la destination d'un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé à haut risque et a déjà été mis sur le marché ou mis en service de telle manière que le système d'IA concerné devient un système d'IA à haut risque conformément l'article 6.

2. Lorsque les circonstances visées au paragraphe 1, se produisent, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA n'est plus considéré comme un fournisseur de ce système d'IA spécifique aux fins du présent règlement. Ce fournisseur initial coopère étroitement avec les nouveaux fournisseurs et met à disposition les informations nécessaires et fournit l'accès technique raisonnablement attendu et toute autre assistance nécessaire au respect des obligations énoncées dans le présent règlement, en particulier en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque. Le présent paragraphe ne s'applique pas dans les cas où le fournisseur initial a clairement précisé que son système d'IA ne doit pas être transformé en un système d'IA à haut risque et ne relève donc pas de l'obligation relative à la remise de la documentation.
3. Lorsque des systèmes d'IA à haut risque constituent des composants de sécurité de produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, le fabricant de ces produits est considéré comme étant le fournisseur du système d'IA à haut risque et est soumis aux obligations visées à l'article 16 dans l'un des deux cas suivants:
 - a) le système d'IA à haut risque est mis sur le marché avec le produit sous le nom ou la marque du fabricant du produit;
 - b) le système d'IA à haut risque est mis en service sous le nom ou la marque du fabricant du produit après que le produit a été mis sur le marché.

4. Le fournisseur d'un système d'IA à haut risque et le tiers qui fournit un système d'IA, des outils, services, composants ou processus qui sont utilisés ou intégrés dans un système d'IA à haut risque précisent, par accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaire, sur la base de l'état de la technique généralement reconnu, pour permettre au fournisseur du système d'IA à haut risque de se conformer pleinement aux obligations prévues dans le présent règlement. Le présent paragraphe ne s'applique pas aux tiers qui rendent accessibles au public des outils, services, processus ou composants, autres que des modèles d'IA à usage général, dans le cadre d'une licence libre et ouverte.

Le Bureau de l'IA peut élaborer et recommander des clauses types volontaires pour les contrats entre les fournisseurs de systèmes d'IA à haut risque et les tiers qui fournissent des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans les systèmes d'IA à haut risque. Lorsqu'il élabore des clauses types volontaires, le Bureau de l'IA tient compte des éventuelles exigences contractuelles applicables dans des secteurs ou des activités spécifiques. Les clauses types volontaires sont publiées et mises à disposition gratuitement dans un format électronique facile d'utilisation.

5. Les paragraphes 2 et 3 sont sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle, les informations confidentielles de nature commerciale et les secrets d'affaires conformément au droit de l'Union et au droit national.

Article 26

Obligations incombant aux déployeurs de systèmes d'IA à haut risque

1. Les déployeurs de systèmes d'IA à haut risque prennent des mesures techniques et organisationnelles appropriées afin de garantir qu'ils utilisent ces systèmes conformément aux notices d'utilisation accompagnant les systèmes, conformément aux paragraphes 3 et 6.

2. Les déployeurs confient le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ainsi que du soutien nécessaire.
3. Les obligations énoncées aux paragraphes 1 et 2 sont sans préjudice des autres obligations du déployeur prévues par le droit de l'Union ou le droit national et de la faculté du déployeur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de contrôle humain indiquées par le fournisseur.
4. Sans préjudice des paragraphes 1 et 2, pour autant que le déployeur exerce un contrôle sur les données d'entrée, il veille à ce que ces dernières soient pertinentes et suffisamment représentatives au regard de la destination du système d'IA à haut risque.
5. Les déployeurs surveillent le fonctionnement du système d'IA à haut risque sur la base de la notice d'utilisation et, le cas échéant, informent les fournisseurs conformément à l'article 72. Lorsque les déployeurs ont des raisons de considérer que l'utilisation du système d'IA à haut risque conformément à la notice d'utilisation pourrait conduire à ce que le système d'IA présente un risque au sens de l'article 79, paragraphe 1, ils en informent, sans retard injustifié, le fournisseur ou le distributeur ainsi que l'autorité de surveillance du marché concernée, et suspendent l'utilisation de ce système. Lorsque les déployeurs ont détecté un incident grave, ils informent également immédiatement d'abord le fournisseur, puis l'importateur ou le distributeur et les autorités de surveillance du marché concernées de cet incident. Si le déployeur n'est pas en mesure de joindre le fournisseur, l'article 73 s'applique mutatis mutandis. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs de systèmes d'IA qui sont des autorités répressives.

Si les déployeurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, la conformité avec les règles relatives à la gouvernance, aux dispositifs, aux processus et aux mécanismes internes prévues dans la législation sur les services financiers vaut respect de l'obligation de surveillance énoncée au premier alinéa.

6. Les déployeurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par ce système d'IA à haut risque dans la mesure où ces journaux se trouvent sous leur contrôle, pendant une période adaptée à la destination du système d'IA à haut risque, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.

Si les déployeurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour les journaux dans le cadre de la documentation conservée en vertu de la législation pertinente de l'Union sur les services financiers.

7. Avant de mettre en service ou d'utiliser un système d'IA à haut risque sur le lieu de travail, les déployeurs qui sont des employeurs informent les représentants des travailleurs et les travailleurs concernés qu'ils seront soumis à l'utilisation du système d'IA à haut risque. Ces informations sont fournies, le cas échéant, conformément aux règles et procédures prévues par le droit de l'Union et le droit national et aux pratiques en matière d'information des travailleurs et de leurs représentants.

8. Les déployeurs de systèmes d'IA à haut risque qui sont des autorités publiques ou des institutions, organes ou organismes de l'Union, respectent les obligations en matière d'enregistrement prévues à l'article 49. Dans le cas où ces déployeurs constatent que le système d'IA à haut risque qu'ils envisagent d'utiliser n'a pas été enregistré dans la base de données de l'UE visée à l'article 71, ils n'utilisent pas ce système et informent le fournisseur ou le distributeur.
9. Le cas échéant, les déployeurs de systèmes d'IA à haut risque utilisent les informations fournies en application de l'article 13 du présent règlement pour se conformer à leur obligation de procéder à une analyse d'impact relative à la protection des données en vertu de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680.
10. Sans préjudice de la directive (UE) 2016/680, dans le cadre d'une enquête en vue de la recherche ciblée d'une personne soupçonnée d'avoir commis une infraction pénale ou condamnée pour avoir commis une infraction pénale, le déployeur d'un système d'IA à haut risque pour l'identification biométrique à distance a posteriori demande l'autorisation, ex ante ou sans retard injustifié et au plus tard dans les 48 heures, d'une autorité judiciaire ou administrative dont la décision est contraignante et soumise à un contrôle juridictionnel, pour l'utilisation de ce système, sauf lorsqu'il est utilisé pour l'identification initiale d'un suspect potentiel sur la base de faits objectifs et vérifiables directement liés à l'infraction. Chaque utilisation est limitée à ce qui est strictement nécessaire pour enquêter sur une infraction pénale spécifique.

Si l'autorisation demandée en application du premier alinéa est rejetée, l'utilisation du système d'identification biométrique à distance a posteriori lié à l'autorisation demandée est interrompue avec effet immédiat et les données à caractère personnel liées à l'utilisation du système d'IA à haut risque pour lequel l'autorisation a été demandée sont supprimées.

En aucun cas, ce système d'IA à haut risque pour l'identification biométrique à distance a posteriori ne peut être utilisé à des fins répressives de manière non ciblée, sans aucun lien avec une infraction pénale, une procédure pénale, une menace réelle et actuelle ou réelle et prévisible d'une infraction pénale, ou la recherche d'une personne disparue spécifique. Il convient d'assurer qu'aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne puisse être prise par les autorités répressives sur la seule base des sorties de tels systèmes d'identification biométrique à distance a posteriori.

Le présent paragraphe est sans préjudice de l'article 9 du règlement (UE) 2016/679 et de l'article 10 de la directive (UE) 2016/680 pour le traitement des données biométriques.

Indépendamment de la finalité ou du déployeur, chaque utilisation de ces systèmes d'IA à haut risque est documentée dans le dossier de police pertinent et est mise à la disposition de l'autorité de surveillance du marché concernée et de l'autorité nationale chargée de la protection des données sur demande, à l'exclusion de la divulgation de données opérationnelles sensibles liées aux services répressifs. Le présent alinéa est sans préjudice des pouvoirs conférés par la directive (UE) 2016/680 aux autorités de contrôle.

Les déployeurs soumettent aux autorités de surveillance du marché concernées et aux autorités nationales chargées de la protection des données des rapports annuels sur leur utilisation de systèmes d'identification biométrique à distance a posteriori, à l'exclusion de la divulgation de données opérationnelles sensibles liées aux services répressifs. Les rapports peuvent être agrégés pour couvrir plus d'un déploiement.

Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance a posteriori.

11. Sans préjudice de l'article 50 du présent règlement, les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, qui prennent des décisions ou facilitent les prises de décision concernant des personnes physiques, informent lesdites personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque. Pour les systèmes d'IA à haut risque utilisés à des fins répressives, l'article 13 de la directive (UE) 2016/680 s'applique.
12. Les déployeurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard du système d'IA à haut risque en vue de mettre en œuvre le présent règlement.

Article 27

Analyse d'impact des systèmes d'IA à haut risque sur les droits fondamentaux

1. Avant le déploiement d'un système d'IA à haut risque visé à l'article 6, paragraphe 2, à l'exception des systèmes d'IA à haut risque destinés à être utilisés dans le domaine visé à l'annexe III, point 2, les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics et les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, points 5) b) et 5) c), effectuent une analyse de l'impact sur les droits fondamentaux que l'utilisation de ce système peut produire. À cette fin, les déployeurs effectuent une analyse comprenant:
 - a) une description des processus du déployeur dans lesquels le système d'IA à haut risque sera utilisé conformément à sa destination;
 - b) une description de la période pendant laquelle et de la fréquence à laquelle chaque système d'IA à haut risque est destiné à être utilisé;

- c) les catégories de personnes physiques et les groupes susceptibles d'être concernés par son utilisation dans le contexte spécifique;
 - d) les risques spécifiques de préjudice susceptibles d'avoir une incidence sur les catégories de personnes physiques ou groupes de personnes identifiés en vertu du point c) du présent paragraphe, compte tenu des informations fournies par le fournisseur conformément à l'article 13;
 - e) une description de la mise en œuvre des mesures de contrôle humain, conformément à la notice d'utilisation;
 - f) les mesures à prendre en cas de matérialisation de ces risques, y compris les dispositifs relatifs à la gouvernance interne et aux mécanismes de plainte internes.
2. L'obligation établie au paragraphe 1 s'applique à la première utilisation du système d'IA à haut risque. Le déployeur peut, dans des cas similaires, s'appuyer sur des analyses d'impact sur les droits fondamentaux effectuées précédemment ou sur des analyses d'impact existantes réalisées par le fournisseur. Si, au cours de l'utilisation du système d'IA à haut risque, le déployeur estime qu'un des éléments énumérés au paragraphe 1 a changé ou n'est plus à jour, il prend les mesures nécessaires pour mettre à jour les informations.
3. Une fois l'analyse visée au paragraphe 1 du présent article effectuée, le déployeur en notifie les résultats à l'autorité de surveillance du marché, et soumet le modèle visé au paragraphe 5 du présent article, rempli, dans le cadre de la notification. Dans le cas visé à l'article 46, paragraphe 1, les déployeurs peuvent être exemptés de cette obligation de notification.

4. Si l'une des obligations prévues au présent article est déjà remplie au moyen de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, l'analyse d'impact sur les droits fondamentaux visée au paragraphe 1 du présent article complète ladite analyse d'impact relative à la protection des données.
5. Le Bureau de l'IA élabore un modèle de questionnaire, y compris au moyen d'un outil automatisé, afin d'aider les déployeurs à se conformer de manière simplifiée aux obligations qui leur incombent en vertu du présent article.

SECTION 4

AUTORITES NOTIFIANTES ET ORGANISMES NOTIFIES

Article 28

Autorités notifiantes

1. Chaque État membre désigne ou établit au moins une autorité notifiante chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle. Ces procédures sont élaborées en coopération entre les autorités notifiantes de tous les États membres.
2. Les États membres peuvent décider que l'évaluation et le contrôle visés au paragraphe 1 doivent être effectués par un organisme national d'accréditation au sens du règlement (CE) n° 765/2008 et conformément à ses dispositions.

3. Les autorités notifiantes sont établies, organisées et gérées de manière à éviter tout conflit d'intérêts avec les organismes d'évaluation de la conformité et à garantir l'objectivité et l'impartialité de leurs activités.
4. Les autorités notifiantes sont organisées de telle sorte que les décisions concernant la notification des organismes d'évaluation de la conformité soient prises par des personnes compétentes différentes de celles qui ont réalisé l'évaluation de ces organismes.
5. Les autorités notifiantes ne proposent ni ne fournissent aucune des activités réalisées par les organismes d'évaluation de la conformité, ni aucun service de conseil sur une base commerciale ou concurrentielle.
6. Les autorités notifiantes garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78.
7. Les autorités notifiantes disposent d'un personnel compétent en nombre suffisant pour la bonne exécution de leurs tâches. Le personnel compétent possède l'expertise nécessaire, le cas échéant, pour sa fonction, dans des domaines tels que les technologies de l'information, l'IA et le droit, y compris le contrôle du respect des droits fondamentaux.

Article 29

Demande de notification d'un organisme d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité soumettent une demande de notification à l'autorité notifiante de l'État membre dans lequel ils sont établis.

2. La demande de notification est accompagnée d'une description des activités d'évaluation de la conformité, du ou des modules d'évaluation de la conformité et des types de systèmes d'IA pour lesquels l'organisme d'évaluation de la conformité se déclare compétent, ainsi que d'un certificat d'accréditation, lorsqu'il existe, délivré par un organisme national d'accréditation qui atteste que l'organisme d'évaluation de la conformité remplit les exigences énoncées à l'article 31.

Tout document en cours de validité relatif à des désignations existantes de l'organisme notifié demandeur en vertu de toute autre législation d'harmonisation de l'Union est ajouté.

3. Lorsque l'organisme d'évaluation de la conformité ne peut pas produire de certificat d'accréditation, il présente à l'autorité notifiante toutes les preuves documentaires nécessaires à la vérification, à la reconnaissance et au contrôle régulier de sa conformité avec les exigences définies à l'article 31.
4. Quant aux organismes notifiés désignés en vertu de toute autre législation d'harmonisation de l'Union, tous les documents et certificats liés à ces désignations peuvent être utilisés à l'appui de leur procédure de désignation au titre du présent règlement, le cas échéant. L'organisme notifié met à jour la documentation visée aux paragraphes 2 et 3 du présent article dès que des changements pertinents interviennent afin de permettre à l'autorité responsable des organismes notifiés de contrôler et de vérifier que toutes les exigences énoncées à l'article 31 demeurent observées.

Article 30
Procédure de notification

1. Les autorités notifiantes ne peuvent notifier que les organismes d'évaluation de la conformité qui ont satisfait aux exigences énoncées à l'article 31.
2. Les autorités notifiantes informent la Commission et les autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission quant à chaque organisme d'évaluation de la conformité visé au paragraphe 1.
3. La notification visée au paragraphe 2 du présent article comprend des informations complètes sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et les types de systèmes d'IA concernés, ainsi que l'attestation de compétence correspondante. Lorsqu'une notification n'est pas fondée sur le certificat d'accréditation visé à l'article 29, paragraphe 2, l'autorité notifiante fournit à la Commission et aux autres États membres les preuves documentaires attestant de la compétence de l'organisme d'évaluation de la conformité et des dispositions prises pour faire en sorte que cet organisme soit régulièrement contrôlé et continue à satisfaire aux exigences énoncées à l'article 31.
4. L'organisme d'évaluation de la conformité concerné ne peut effectuer les activités propres à un organisme notifié que si aucune objection n'est émise par la Commission ou les autres États membres dans les deux semaines suivant la notification par une autorité notifiante, si cette notification comprend le certificat d'accréditation visé à l'article 29, paragraphe 2, ou dans les deux mois suivant la notification par une autorité notifiante si cette notification comprend les preuves documentaires visées à l'article 29, paragraphe 3.

5. En cas d'objections, la Commission entame sans tarder des consultations avec les États membres et l'organisme d'évaluation de la conformité concernés. Au vu de ces consultations, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre et à l'organisme d'évaluation de la conformité concernés.

Article 31

Exigences concernant les organismes notifiés

1. Un organisme notifié est constitué en vertu du droit national d'un État membre et a la personnalité juridique.
2. Les organismes notifiés se conforment aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de procédures qui sont nécessaires à l'exécution de leurs tâches, ainsi qu'aux exigences appropriées en matière de cybersécurité.
3. La structure organisationnelle, la répartition des responsabilités, les liens hiérarchiques et le fonctionnement des organismes notifiés garantissent la confiance dans leurs activités et la fiabilité des résultats des activités d'évaluation de la conformité menées par les organismes notifiés.
4. Les organismes notifiés sont indépendants du fournisseur du système d'IA à haut risque pour lequel ils mènent les activités d'évaluation de la conformité. Les organismes notifiés sont également indépendants de tout autre opérateur ayant un intérêt économique dans les systèmes d'IA à haut risque qui font l'objet de l'évaluation, ainsi que de tout concurrent du fournisseur. Cela n'exclut pas l'utilisation de systèmes d'IA à haut risque évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces systèmes d'IA à haut risque à des fins personnelles.

5. L'organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter ses tâches d'évaluation de la conformité ne participent pas directement à la conception, au développement, à la commercialisation ou à l'utilisation de systèmes d'IA à haut risque, pas plus qu'ils ne représentent les parties engagées dans ces activités. Ils n'exercent aucune activité susceptible d'entrer en conflit avec leur indépendance de jugement ou leur intégrité en ce qui concerne les activités d'évaluation de la conformité pour lesquelles ils sont notifiés. Cela s'applique en particulier aux services de conseil.
6. Les organismes notifiés sont organisés et fonctionnent de façon à garantir l'indépendance, l'objectivité et l'impartialité de leurs activités. Les organismes notifiés documentent et appliquent une structure et des procédures visant à garantir l'impartialité et à encourager et appliquer les principes d'impartialité dans l'ensemble de leur organisation, du personnel et des activités d'évaluation.
7. Les organismes notifiés disposent de procédures documentées pour veiller à ce que leur personnel, leurs comités, leurs filiales, leurs sous-traitants et tout organisme associé ou le personnel d'organismes externes préservent, conformément à l'article 78, la confidentialité des informations auxquelles ils accèdent durant l'exercice de leurs activités d'évaluation de la conformité, sauf lorsque leur divulgation est requise par la loi. Le personnel des organismes notifiés est lié par le secret professionnel pour toutes les informations dont il a connaissance dans l'exercice de ses fonctions au titre du présent règlement, sauf à l'égard des autorités notifiantes de l'État membre où il exerce ses activités.

8. Les organismes notifiés disposent de procédures pour accomplir leurs activités qui tiennent dûment compte de la taille des fournisseurs, du secteur dans lequel ils exercent leurs activités, de leur structure et du degré de complexité du système d'IA concerné.
9. Les organismes notifiés souscrivent, pour leurs activités d'évaluation de la conformité, une assurance de responsabilité civile appropriée à moins que cette responsabilité ne soit couverte par l'État membre dans lequel ils sont établis sur la base du droit national ou que l'État membre soit lui-même responsable de l'évaluation de la conformité.
10. Les organismes notifiés sont en mesure d'accomplir toutes leurs tâches au titre du présent règlement avec la plus haute intégrité professionnelle et la compétence requise dans le domaine spécifique, qu'ils exécutent eux-mêmes ces tâches ou que celles-ci soient exécutées pour leur compte et sous leur responsabilité.
11. Les organismes notifiés disposent de compétences internes suffisantes pour pouvoir évaluer efficacement les tâches effectuées pour leur compte par des parties extérieures. L'organisme notifié dispose en permanence d'un personnel administratif, technique, juridique et scientifique en nombre suffisant et doté d'une expérience et de connaissances liées aux données, au traitement des données et aux types de systèmes d'IA en cause et aux exigences énoncées à la section 2.
12. Les organismes notifiés prennent part aux activités de coordination visées à l'article 38. Ils participent également, directement ou par l'intermédiaire d'un représentant, aux activités des organisations européennes de normalisation, ou font en sorte de se tenir informés des normes applicables et de leur état.

Article 32

Présomption de conformité avec les exigences concernant les organismes notifiés

Lorsqu'un organisme d'évaluation de la conformité démontre sa conformité avec les critères énoncés dans les normes harmonisées concernées, ou dans des parties de ces normes, dont les références ont été publiées au *Journal officiel de l'Union européenne*, il est présumé répondre aux exigences énoncées à l'article 31 dans la mesure où les normes harmonisées applicables couvrent ces exigences.

Article 33

Filiales des organismes notifiés et sous-traitance

1. Lorsqu'un organisme notifié sous-traite des tâches spécifiques dans le cadre de l'évaluation de la conformité ou a recours à une filiale, il s'assure que le sous-traitant ou la filiale répond aux exigences fixées à l'article 31 et en informe l'autorité notifiante.
2. Les organismes notifiés assument l'entière responsabilité des tâches effectuées par tout sous-traitants ou toute filiale.
3. Des activités ne peuvent être sous-traitées ou réalisées par une filiale qu'avec l'accord du fournisseur. Les organismes notifiés rendent publique une liste de leurs filiales.
4. Les documents pertinents concernant l'évaluation des qualifications du sous-traitant ou de la filiale et le travail exécuté par celui-ci ou celle-ci en vertu du présent règlement sont tenus à la disposition de l'autorité notifiante pendant une période de cinq ans à compter de la date de cessation de la sous-traitance.

Article 34

Obligations opérationnelles des organismes notifiés

1. Les organismes notifiés vérifient la conformité du système d'IA à haut risque conformément aux procédures d'évaluation de la conformité visées à l'article 43.
2. Les organismes notifiés évitent les charges inutiles pour les fournisseurs dans l'exercice de leurs activités et tiennent dûment compte de la taille du fournisseur, du secteur dans lequel il exerce ses activités, de sa structure et du degré de complexité du système d'IA à haut risque concerné, en particulier en vue de réduire au minimum les charges administratives et les coûts de mise en conformité pour les microentreprises et les petites entreprises au sens de la recommandation 2003/361/CE. L'organisme notifié respecte néanmoins le degré de rigueur et le niveau de protection requis afin de garantir la conformité du système d'IA à haut risque avec les exigences du présent règlement.
3. Les organismes notifiés mettent à la disposition de l'autorité notifiante visée à l'article 28 et lui soumettent sur demande toute la documentation pertinente, y compris celle des fournisseurs, afin de permettre à cette autorité de réaliser ses activités d'évaluation, de désignation, de notification et de surveillance et pour faciliter les évaluations décrites à la présente section.

Article 35

Numéros d'identification et listes des organismes notifiés

1. La Commission attribue un numéro d'identification unique à chaque organisme notifié, même lorsqu'un organisme est notifié au titre de plus d'un acte de l'Union.

2. La Commission rend publique la liste des organismes notifiés au titre du présent règlement et y mentionne leurs numéros d'identification et les activités pour lesquelles ils ont été notifiés. La Commission veille à ce que cette liste soit tenue à jour.

Article 36

Modifications apportées aux notifications

1. L'autorité notifiante notifie à la Commission et aux autres États membres toute modification pertinente apportée à la notification d'un organisme notifié au moyen de l'outil de notification électronique visé à l'article 30, paragraphe 2.
2. Les procédures établies aux articles 29 et 30 s'appliquent en cas d'extension de la portée de la notification.

En cas de modification de la notification autre qu'une extension de sa portée, les procédures prévues aux paragraphes 3 à 9 s'appliquent.

3. Lorsqu'un organisme notifié décide de cesser ses activités d'évaluation de la conformité, il informe l'autorité notifiante et les fournisseurs concernés dès que possible et, dans le cas d'un arrêt prévu de ses activités, au moins un an avant de mettre un terme à ses activités. Les certificats de l'organisme notifié peuvent rester valables pendant une période de neuf mois après l'arrêt des activités de l'organisme notifié, à condition qu'un autre organisme notifié confirme par écrit qu'il assumera la responsabilité des systèmes d'IA à haut risque concernés par ces certificats. Cet autre organisme notifié procède à une évaluation complète des systèmes d'IA à haut risque concernés avant la fin de cette période de neuf mois, avant de délivrer de nouveaux certificats pour les systèmes en question. Lorsque l'organisme notifié a mis un terme à ses activités, l'autorité notifiante retire la désignation.

4. Lorsqu'une autorité notifiante a des raisons suffisantes de considérer qu'un organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, l'autorité notifiante procède sans retard à une enquête avec la plus grande diligence. Dans ce contexte, elle informe l'organisme notifié concerné des objections soulevées et lui donne la possibilité de faire connaître son point de vue. Si l'autorité notifiante conclut que l'organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, elle soumet la désignation à des restrictions, la suspend ou la retire, selon le cas, en fonction de la gravité du manquement. Elle en informe immédiatement la Commission et les autres États membres.
5. Lorsque sa désignation a été suspendue, restreinte ou révoquée en tout ou en partie, l'organisme notifié en informe les fournisseurs concernés dans un délai de dix jours.
6. En cas de restriction, de suspension ou de retrait d'une désignation, l'autorité notifiante prend les mesures nécessaires pour que les dossiers de l'organisme notifié en question soient conservés et pour qu'ils soient mis à la disposition des autorités notifiantes d'autres États membres et des autorités de surveillance du marché, à leur demande.
7. En cas de restriction, de suspension ou de retrait d'une désignation, l'autorité notifiante:
 - a) évalue l'incidence sur les certificats délivrés par l'organisme notifié;
 - b) transmet un rapport sur ses conclusions à la Commission et aux autres États membres dans un délai de trois mois après avoir signalé les modifications apportées à la désignation;

- c) exige de l'organisme notifié qu'il suspende ou retire, dans un délai raisonnable qu'elle détermine, tous les certificats délivrés à tort afin d'assurer la conformité constante des systèmes d'IA à haut risque sur le marché;
 - d) informe la Commission et les États membres des certificats dont elle a demandé la suspension ou le retrait;
 - e) fournit aux autorités nationales compétentes de l'État membre dans lequel le fournisseur a son siège social toutes les informations pertinentes sur les certificats dont elle a demandé la suspension ou le retrait; cette autorité prend les mesures appropriées si cela est nécessaire pour éviter un risque potentiel pour la santé, la sécurité ou les droits fondamentaux.
8. À l'exception des certificats délivrés à tort, et lorsqu'une désignation a été suspendue ou restreinte, les certificats restent valables dans l'un des cas suivants:
- a) l'autorité notifiante a confirmé, dans un délai d'un mois suivant la suspension ou la restriction, qu'il n'y a pas de risque pour la santé, la sécurité ou les droits fondamentaux en lien avec les certificats concernés par la suspension ou la restriction, et l'autorité notifiante a défini un calendrier de mesures pour remédier à la suspension ou à la restriction; ou

b) l'autorité notifiante a confirmé qu'aucun certificat ayant trait à la suspension ne sera délivré, modifié ou délivré à nouveau pendant la période de suspension ou de restriction et elle indique si l'organisme notifié est en mesure de continuer à contrôler les certificats existants délivrés et à en être responsable pour la durée de la suspension ou de la restriction. Si l'autorité notifiante considère que l'organisme notifié n'est pas en mesure de se charger des certificats existants délivrés, le fournisseur du système faisant l'objet du certificat confirme par écrit aux autorités nationales compétentes de l'État membre dans lequel il a son siège social, dans un délai de trois mois suivant la suspension ou la restriction, qu'un autre organisme notifié qualifié assume temporairement les fonctions de surveillance de l'organisme notifié et continue d'assumer la responsabilité des certificats pour la durée de la suspension ou de la restriction.

9. À l'exception des certificats délivrés à tort, et lorsqu'une désignation a été retirée, les certificats restent valables pendant une durée de neuf mois dans les cas suivants:

- a) l'autorité nationale compétente de l'État membre dans lequel le fournisseur du système d'IA à haut risque faisant l'objet du certificat a son siège social a confirmé que les systèmes d'IA à haut risque en question ne présentent pas de risque pour la santé, la sécurité ou les droits fondamentaux; et
- b) un autre organisme notifié a confirmé par écrit qu'il assumera la responsabilité immédiate de ces systèmes d'IA et achèvera son évaluation dans un délai de douze mois à compter du retrait de la désignation.

Dans le cas visé au premier alinéa, l'autorité nationale compétente de l'État membre dans lequel le fournisseur du système faisant l'objet du certificat a son siège peut prolonger à plusieurs reprises la durée de validité provisoire des certificats de trois mois supplémentaires, pour une durée totale maximale de douze mois.

L'autorité nationale compétente ou l'organisme notifié assumant les fonctions de l'organisme notifié concerné par la modification de la désignation en informe immédiatement la Commission, les autres États membres et les autres organismes notifiés.

Article 37

Contestation de la compétence des organismes notifiés

1. La Commission enquête, s'il y a lieu, sur tous les cas où il existe des raisons de douter de la compétence d'un organisme notifié ou du respect continu, par un organisme notifié, des exigences établies à l'article 31 et de ses responsabilités applicables.
2. L'autorité notifiante fournit à la Commission, sur demande, toutes les informations utiles relatives à la notification ou au maintien de la compétence de l'organisme notifié concerné.
3. La Commission veille à ce que toutes les informations sensibles obtenues au cours des enquêtes qu'elle mène au titre du présent article soient traitées de manière confidentielle conformément à l'article 78.

4. Lorsque la Commission établit qu'un organisme notifié ne répond pas ou ne répond plus aux exigences relatives à sa notification, elle informe l'État membre notifiant en conséquence et lui demande de prendre les mesures correctives qui s'imposent, y compris la suspension ou le retrait de la notification si nécessaire. Si l'État membre ne prend pas les mesures correctives qui s'imposent, la Commission peut, au moyen d'un acte d'exécution, suspendre, restreindre ou retirer la désignation. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 38

Coordination des organismes notifiés

1. La Commission veille à ce que, en ce qui concerne les systèmes d'IA à haut risque, une coordination et une coopération appropriées entre les organismes notifiés intervenant dans les procédures d'évaluation de la conformité conformément au présent règlement soient mises en place et gérées de manière adéquate dans le cadre d'un groupe sectoriel d'organismes notifiés.
2. Chaque autorité notifiante veille à ce que les organismes qu'elle a notifiés participent aux travaux d'un groupe visé au paragraphe 1, directement ou par l'intermédiaire de représentants désignés.
3. La Commission veille à l'échange des connaissances et des bonnes pratiques entre les autorités notifiantes.

Article 39

Organismes d'évaluation de la conformité de pays tiers

Les organismes d'évaluation de la conformité établis conformément à la législation d'un pays tiers avec lequel l'Union a conclu un accord peuvent être autorisés à exercer les activités d'organismes notifiés au titre du présent règlement, pour autant qu'ils répondent aux exigences prévues à l'article 31 ou qu'ils veillent à un niveau équivalent de respect.

SECTION 5

NORMES, EVALUATION DE LA CONFORMITE, CERTIFICATS, ENREGISTREMENT

Article 40

Normes harmonisées et travaux de normalisation

1. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* conformément au règlement (UE) 1025/2012 sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, du présent règlement, dans la mesure où ces exigences ou obligations sont couvertes par ces normes.

2. Conformément à l'article 10 du règlement (UE) n° 1025/2012, la Commission présente sans retard injustifié des demandes de normalisation couvrant toutes les exigences énoncées à la section 2 du présent chapitre et, le cas échéant, les demandes de normalisation couvrant les obligations énoncées au chapitre V, sections 2 et 3, du présent règlement. La demande de normalisation inclut également une demande de livrables sur les processus de déclaration et de documentation afin d'améliorer les performances des systèmes d'IA en matière de ressources, telles que la réduction de la consommation d'énergie et d'autres ressources par le système d'IA à haut risque au cours de son cycle de vie, et sur le développement économe en énergie de modèles d'IA à usage général. Lors de la préparation d'une demande de normalisation, la Commission consulte le Comité IA et les parties prenantes concernées, y compris le forum consultatif.

Lorsqu'elle présente une demande de normalisation aux organisations européennes de normalisation, la Commission précise que les normes doivent être claires, cohérentes, y compris avec les normes développées dans les différents secteurs pour les produits relevant de la législation d'harmonisation de l'Union existante dont la liste figure à l'annexe I, et visant à veiller à ce que les systèmes d'IA à haut risque ou les modèles d'IA à usage général mis sur le marché ou mis en service dans l'Union satisfont aux exigences ou obligations pertinentes énoncées dans le présent règlement.

La Commission demande aux organisations européennes de normalisation de fournir la preuve qu'elles mettent tout en œuvre pour atteindre les objectifs visés aux premier et deuxième alinéas du présent paragraphe, conformément à l'article 24 du règlement (UE) n° 1025/2012.

3. Les participants au processus de normalisation s'efforcent de favoriser les investissements et l'innovation dans le domaine de l'IA, y compris en renforçant la sécurité juridique, ainsi que la compétitivité et la croissance du marché de l'Union, de contribuer à renforcer la coopération mondiale en faveur d'une normalisation en tenant compte des normes internationales existantes dans le domaine de l'IA qui sont conformes aux valeurs et aux intérêts de l'Union et aux droits fondamentaux, et de renforcer la gouvernance multipartite en veillant à une représentation équilibrée des intérêts et à la participation effective de toutes les parties prenantes concernées conformément aux articles 5, 6 et 7 du règlement (UE) n° 1025/2012.

Article 41

Spécifications communes

1. La Commission peut adopter des actes d'exécution établissant des spécifications communes pour les exigences énoncées à la section 2 du présent chapitre ou, le cas échéant, pour les obligations énoncées au chapitre IV, sections 2 et 3, lorsque les conditions suivantes sont remplies:
 - a) la Commission, en vertu de l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012, a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée pour les exigences énoncées à la section 2 du présent chapitre ou, le cas échéant, pour les obligations énoncées au chapitre V, sections 2 et 3, et:
 - i) la demande n'a été acceptée par aucune des organisations européennes de normalisation; ou

- ii) les normes harmonisées faisant l'objet de cette demande n'ont pas été présentées dans le délai fixé conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012; ou
 - iii) les normes harmonisées pertinentes ne répondent pas suffisamment aux préoccupations en matière de droits fondamentaux; ou
 - iv) les normes harmonisées ne sont pas conformes à la demande; et
- b) aucune référence à des normes harmonisées couvrant les exigences visées à la section 2 du chapitre ou, le cas échéant, les obligations énoncées au chapitre V, sections 2 et 3, n'a été publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012, et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Lors de la rédaction des spécifications communes, la Commission consulte le forum consultatif visé à l'article 67.

Les actes d'exécution visés au premier alinéa du présent paragraphe sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Avant d'élaborer un projet d'acte d'exécution, la Commission informe le comité visé à l'article 22 du règlement (UE) n° 1025/2012 qu'elle considère que les conditions énoncées au paragraphe 1 du présent article sont remplies.

3. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes aux spécifications communes visées au paragraphe 1, ou à des parties de ces spécifications, sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant pour se conformer aux obligations visées au chapitre V, sections 2 et 3, dans la mesure où ces exigences ou obligations sont couvertes par ces spécifications communes.
4. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au *Journal officiel de l'Union européenne*, la Commission procède à l'évaluation de cette norme harmonisée conformément au règlement (UE) n° 1025/2012. Lorsque la référence à une norme harmonisée est publiée au *Journal officiel de l'Union européenne*, la Commission abroge les actes d'exécution visés au paragraphe 1, ou les parties de ces actes qui couvrent les mêmes exigences que celles énoncées à la section 2 du présent chapitre ou, le cas échéant les mêmes obligations que celles énoncées au chapitre V, sections 2 et 3.
5. Lorsque les fournisseurs de systèmes d'IA à haut risque ou de modèles d'IA à usage général ne respectent pas les spécifications communes visées au paragraphe 1, ils justifient dûment avoir adopté des solutions techniques qui satisfont aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, à un niveau au moins équivalent auxdites spécifications.

6. Lorsqu'un État membre considère qu'une spécification commune ne satisfait pas entièrement aux exigences énoncées à la section 2 ou, le cas échéant aux obligations énoncées au chapitre V, sections 2 et 3, il en informe la Commission au moyen d'une explication détaillée. La Commission évalue ces informations et, le cas échéant, modifie l'acte d'exécution établissant la spécification commune concernée.

Article 42

Présomption de conformité avec certaines exigences

1. Les systèmes d'IA à haut risque qui ont été entraînés et testés avec des données tenant compte du cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel ils sont destinés à être utilisés sont présumés conformes aux exigences pertinentes établies à l'article 10, paragraphe 4.
2. Les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au règlement (UE) 2019/881 et dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences de cybersécurité énoncées à l'article 15 du présent règlement, dans la mesure où ces dernières sont couvertes par tout ou partie du certificat de cybersécurité ou de la déclaration de conformité.

Article 43
Évaluation de la conformité

1. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, lorsque, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, le fournisseur a appliqué les normes harmonisées visées à l'article 40 ou, le cas échéant, les spécifications communes visées à l'article 41, il choisit l'une des procédures d'évaluation de la conformité suivantes sur la base:
 - a) du contrôle interne visé à l'annexe VI; ou
 - b) de l'évaluation du système de gestion de la qualité et de l'évaluation de la documentation technique, avec l'intervention d'un organisme notifié, visée à l'annexe VII.

Pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, le fournisseur suit la procédure d'évaluation de la conformité prévue à l'annexe VII dans les cas suivants:

- a) les normes harmonisées visées à l'article 40 n'existent pas et les spécifications communes visées à l'article 41 font défaut;
- b) le fournisseur n'a pas appliqué la norme harmonisée ou ne l'a appliquée que partiellement;
- c) les spécifications communes visées au point a) existent, mais le fournisseur ne les a pas appliquées;

- d) une ou plusieurs des normes harmonisées visées au point a), ont été publiées assorties d'une restriction et seulement sur la partie de la norme qui a été soumise à une restriction.

Aux fins de la procédure d'évaluation de la conformité visée à l'annexe VII, le fournisseur peut choisir n'importe lequel des organismes notifiés. Toutefois, lorsque le système d'IA à haut risque est destiné à être mis en service par les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile ou par les institutions, organes ou organismes de l'UE, l'autorité de surveillance du marché visée à l'article 74, paragraphe 8 ou 9, selon le cas, agit en tant qu'organisme notifié.

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI, qui ne prévoit pas d'intervention d'un organisme notifié.
3. Pour les systèmes d'IA à haut risque couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, le fournisseur suit la procédure d'évaluation de la conformité pertinente selon les modalités requises par ces actes juridiques. Les exigences énoncées à la section 2 du présent chapitre s'appliquent à ces systèmes d'IA à haut risque et font partie de cette évaluation. Les points 4.3, 4.4 et 4.5 de l'annexe VII ainsi que le point 4.6, cinquième alinéa, de ladite annexe s'appliquent également.

Aux fins de ces évaluations, les organismes notifiés qui ont été notifiés en vertu de ces actes juridiques sont habilités à contrôler la conformité des systèmes d'IA à haut risque avec les exigences énoncées à la section 2, à condition que le respect, par ces organismes notifiés, des exigences énoncées à l'article 31, paragraphes 4, 10 et 11, ait été évalué dans le cadre de la procédure de notification prévue par ces actes juridiques.

Lorsqu'un acte juridique énuméré à l'annexe I, section A, confère au fabricant du produit la faculté de ne pas faire procéder à une évaluation de la conformité par un tiers, à condition que ce fabricant ait appliqué toutes les normes harmonisées couvrant toutes les exigences pertinentes, ce fabricant ne peut faire usage de cette faculté que s'il a également appliqué les normes harmonisées ou, le cas échéant, les spécifications communes visées à l'article 41 couvrant toutes les exigences énoncées à la section 2 du présent chapitre.

4. Les systèmes d'IA à haut risque qui ont déjà été soumis à une procédure d'évaluation de la conformité sont soumis à une nouvelle procédure d'évaluation de la conformité lorsqu'ils font l'objet de modifications substantielles, que le système modifié soit destiné à être distribué plus largement ou reste utilisé par le dépoyeur actuel.

Pour les systèmes d'IA à haut risque qui continuent leur apprentissage après avoir été mis sur le marché ou mis en service, les modifications apportées au système d'IA à haut risque et à sa performance qui ont été déterminées au préalable par le fournisseur au moment de l'évaluation initiale de la conformité et font partie des informations contenues dans la documentation technique visée à l'annexe IV, point 2) f), ne constituent pas une modification substantielle.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier les annexes VI et VII afin de les mettre à jour compte tenu du progrès technique.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier les paragraphes 1 et 2 du présent article afin de soumettre les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, à tout ou partie de la procédure d'évaluation de la conformité visée à l'annexe VII. La Commission adopte ces actes délégués en tenant compte de l'efficacité de la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI pour prévenir ou réduire au minimum les risques que ces systèmes font peser sur la santé et la sécurité et sur la protection des droits fondamentaux, ainsi que de la disponibilité de capacités et de ressources suffisantes au sein des organismes notifiés.

Article 44

Certificats

1. Les certificats délivrés par les organismes notifiés conformément à l'annexe VII sont établis dans une langue aisément compréhensible par les autorités compétentes de l'État membre dans lequel l'organisme notifié est établi.
2. Les certificats sont valables pendant la période indiquée sur ceux-ci, qui n'excède pas cinq ans pour les systèmes d'IA relevant de l'annexe I, et quatre ans pour les systèmes d'IA relevant de l'annexe III. À la demande du fournisseur, la durée de validité d'un certificat peut être prolongée d'une durée maximale de cinq ans à chaque fois pour les systèmes d'IA relevant de l'annexe I, et de quatre ans pour les systèmes d'IA relevant de l'annexe III, sur la base d'une nouvelle évaluation suivant les procédures d'évaluation de la conformité applicables. Tout document complémentaire à un certificat reste valable, à condition que le certificat qu'il complète le soit.

3. Lorsqu'un organisme notifié constate qu'un système d'IA ne répond plus aux exigences énoncées à la section 2, il suspend ou retire le certificat délivré ou l'assortit de restrictions, en tenant compte du principe de proportionnalité, sauf si le fournisseur applique, en vue du respect de ces exigences, des mesures correctives appropriées dans le délai imparti à cet effet par l'organisme notifié. L'organisme notifié motive sa décision.

Une procédure de recours contre les décisions des organismes notifiés, y compris concernant des certificats de conformité délivrés, est disponible.

Article 45

Obligations d'information des organismes notifiés

1. Les organismes notifiés communiquent à l'autorité notifiante:
 - a) tout certificat d'évaluation UE de la documentation technique, tout document complémentaire afférent à ce certificat, et toute approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;
 - b) tout refus, restriction, suspension ou retrait d'un certificat d'évaluation UE de la documentation technique ou d'une approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;
 - c) toute circonstance ayant une incidence sur la portée ou les conditions de la notification;

- d) toute demande d'information reçue des autorités de surveillance du marché concernant les activités d'évaluation de la conformité;
 - e) sur demande, les activités d'évaluation de la conformité réalisées dans le cadre de leur notification et toute autre activité réalisée, y compris les activités transfrontières et sous-traitées.
2. Chaque organisme notifié porte à la connaissance des autres organismes notifiés:
- a) les approbations de systèmes de gestion de la qualité qu'il a refusées, suspendues ou retirées et, sur demande, les approbations qu'il a délivrées;
 - b) les certificats d'évaluation UE de la documentation technique ou les documents complémentaires y afférents qu'il a refusés, retirés, suspendus ou soumis à d'autres restrictions et, sur demande, les certificats et/ou documents complémentaires y afférents qu'il a délivrés.
3. Chaque organisme notifié fournit aux autres organismes notifiés qui accomplissent des activités similaires d'évaluation de la conformité portant sur les mêmes types de systèmes d'IA des informations pertinentes sur les aspects liés à des résultats négatifs et, sur demande, à des résultats positifs d'évaluation de la conformité.
4. Les autorités notifiantes garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78.

Article 46

Dérogation à la procédure d'évaluation de la conformité

1. Par dérogation à l'article 43 et sur demande dûment justifiée, toute autorité de surveillance du marché peut, pour des raisons exceptionnelles de sécurité publique ou pour assurer la protection de la vie et de la santé humaines, la protection de l'environnement ou la protection d'actifs industriels et d'infrastructures d'importance majeure, autoriser la mise sur le marché ou la mise en service de systèmes d'IA à haut risque spécifiques sur le territoire de l'État membre concerné. Cette autorisation est accordée pour une période limitée pendant la durée des procédures d'évaluation de la conformité nécessaires, en tenant compte des raisons exceptionnelles justifiant la dérogation. Ces procédures sont menées à bien sans retard injustifié.
2. Dans une situation d'urgence dûment justifiée pour des raisons exceptionnelles de sécurité publique ou en cas de menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques, les autorités répressives ou les autorités de protection civile peuvent mettre en service un service d'IA à haut risque spécifique sans avoir obtenu l'autorisation visée au paragraphe 1, à condition que cette autorisation soit demandée sans retard injustifié pendant ou après l'utilisation. Si l'autorisation visée au paragraphe 1 est refusée, l'utilisation du système d'IA à haut risque cesse immédiatement et tous les résultats et sorties de cette utilisation sont immédiatement mis au rebut.

3. L'autorisation visée au paragraphe 1 n'est délivrée que si l'autorité de surveillance du marché conclut que le système d'IA à haut risque satisfait aux exigences de la section 2. L'autorité de surveillance du marché informe la Commission et les autres États membres de toute autorisation délivrée conformément aux paragraphes 1 et 2. Cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives.
4. Si aucune objection n'est émise, dans un délai de quinze jours civils suivant la réception des informations visées au paragraphe 3, par un État membre ou par la Commission à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un État membre conformément au paragraphe 1, cette autorisation est réputée justifiée.
5. Si, dans un délai de quinze jours civils suivant la réception de la notification visée au paragraphe 3, un État membre soulève des objections à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un autre État membre, ou si la Commission estime que l'autorisation est contraire au droit de l'Union ou que la conclusion des États membres quant à la conformité du système visée au paragraphe 3 n'est pas fondée, la Commission entame sans retard des consultations avec l'État membre concerné. Les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Sur cette base, la Commission décide si l'autorisation est justifiée ou non. La Commission communique sa décision à l'État membre concerné ainsi qu'aux opérateurs concernés.
6. Si la Commission estime que l'autorisation est injustifiée, elle est retirée par l'autorité de surveillance du marché de l'État membre concerné.

7. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, seules les dérogations à l'évaluation de la conformité établies dans ladite législation d'harmonisation de l'Union s'appliquent.

Article 47

Déclaration UE de conformité

1. Le fournisseur établit une déclaration UE de conformité écrite, lisible par machine, signée à la main ou électroniquement concernant chaque système d'IA à haut risque et la tient à la disposition des autorités nationales compétentes pendant une durée de dix ans à partir du moment où le système d'IA à haut risque a été mis sur le marché ou mis en service. La déclaration UE de conformité identifie le système d'IA à haut risque pour lequel elle a été établie. Une copie de la déclaration UE de conformité est communiquée, sur demande, aux autorités nationales compétentes concernées.
2. La déclaration UE de conformité atteste que le système d'IA à haut risque concerné satisfait aux exigences énoncées à la section 2. La déclaration UE de conformité contient les informations qui figurent à l'annexe V et est traduite dans une langue aisément compréhensible par les autorités nationales compétentes des États membres dans lesquels le système d'IA à haut risque est mis sur le marché ou mis à disposition.

3. Si des systèmes d'IA à haut risque sont soumis à d'autres actes législatifs d'harmonisation de l'Union qui exigent également une déclaration UE de conformité, une seule déclaration UE de conformité est établie au titre de tous les actes législatifs de l'Union applicables au système d'IA à haut risque. La déclaration contient toutes les informations nécessaires à l'identification de la législation d'harmonisation de l'Union à laquelle la déclaration se rapporte.
4. Lors de l'établissement de la déclaration UE de conformité, le fournisseur assume la responsabilité du respect des exigences énoncées à la section 2. Le fournisseur tient à jour la déclaration UE de conformité, le cas échéant.
5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe V en mettant à jour le contenu de la déclaration UE de conformité prévu à ladite annexe afin d'y introduire les éléments devenus nécessaires compte tenu du progrès technique.

Article 48

Marquage CE

1. Le marquage CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) n° 765/2008.
2. Pour les systèmes d'IA à haut risque fournis numériquement, un marquage CE numérique n'est utilisé que s'il est facile d'y accéder par l'interface à partir de laquelle l'accès à ce système s'effectue ou au moyen d'un code facilement accessible lisible par machine ou d'autres moyens électroniques.

3. Le marquage CE est apposé de façon visible, lisible et indélébile sur les systèmes d'IA à haut risque. Si cela est impossible ou injustifié étant donné la nature du système d'IA à haut risque, il est apposé sur l'emballage ou sur les documents d'accompagnement, selon le cas.
4. Le cas échéant, le marquage CE est suivi du numéro d'identification de l'organisme notifié responsable des procédures d'évaluation de la conformité prévues à l'article 43. Le numéro d'identification de l'organisme notifié est apposé par l'organisme lui-même ou, sur instruction de celui-ci, par le fournisseur ou par le mandataire du fournisseur. Le numéro d'identification est également indiqué dans tous les documents publicitaires mentionnant que le système d'IA à haut risque est conforme aux exigences applicables au marquage CE.
5. Lorsque des systèmes d'IA à haut risque sont soumis à d'autres actes législatifs de l'Union qui prévoient aussi l'apposition du marquage CE, ce marquage indique que les systèmes d'IA à haut risque satisfont également aux exigences de ces autres actes législatifs.

Article 49

Enregistrement

1. Avant de mettre sur le marché ou de mettre en service un système d'IA à haut risque énuméré à l'annexe III, à l'exception des systèmes d'IA à haut risque visés à l'annexe III, point 2, le fournisseur ou, selon le cas, le mandataire s'enregistre dans la base de données de l'UE visée à l'article 71 et y enregistre aussi son système.

2. Avant de mettre sur le marché ou de mettre en service un système d'IA à propos duquel le fournisseur a conclu qu'il ne s'agissait pas d'un système à haut risque au titre de l'article 6, paragraphe 3, ce fournisseur ou, selon le cas, le mandataire s'enregistre dans la base de données de l'UE visée à l'article 71 et y enregistre aussi ce système.
3. Avant de mettre en service ou d'utiliser un système d'IA à haut risque énuméré à l'annexe III, à l'exception des systèmes d'IA à haut risque énumérés à l'annexe III, point 2, les déployeurs qui sont des autorités publiques, des institutions organes ou organismes de l'Union ou des personnes agissant en leur nom s'enregistrent, sélectionnent le système et enregistrent son utilisation dans la base de données de l'UE visée à l'article 71.
4. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, l'enregistrement visé aux paragraphes 1, 2 et 3 du présent article figure dans une section sécurisée non publique de la base de données de l'UE visée à l'article 71 et comprend uniquement les informations suivantes, selon le cas, visées:
 - a) à l'annexe VIII, section A, points 1 à 10, à l'exception des points 6, 8 et 9;
 - b) à l'annexe VIII, section B, points 1 à 5, et points 8 et 9;
 - c) à l'annexe VIII, section C, points 1 à 3;
 - d) à l'annexe IX, points 1, 2, 3 et 5.

Seules la Commission et les autorités nationales visées à l'article 74, paragraphe 8, ont accès aux différentes sections restreintes de la base de données de l'UE énumérées au premier alinéa du présent paragraphe.

5. Les systèmes d'IA à haut risque visés à l'annexe III, point 2, sont enregistrés au niveau national.

Chapitre IV

Obligations de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA

Article 50

Obligations de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA

1. Les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir directement avec des personnes physiques soient conçus et développés de manière à ce que les personnes physiques concernées soient informées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation. Cette obligation ne s'applique pas aux systèmes d'IA dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers, sauf si ces systèmes sont mis à la disposition du public pour permettre le signalement d'une infraction pénale.

2. Les fournisseurs de systèmes d'IA, y compris de systèmes d'IA à usage général, qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA. Les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet, compte tenu des spécificités et des limites des différents types de contenus, des coûts de mise en œuvre et de l'état de la technique généralement reconnu, comme cela peut ressortir des normes techniques pertinentes. Cette obligation ne s'applique pas dans la mesure où les systèmes d'IA remplissent une fonction d'assistance pour la mise en forme standard ou ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique, ou lorsque leur utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière.
3. Les déployeurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique informent les personnes physiques qui y sont exposées du fonctionnement du système et traitent les données à caractère personnel conformément au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive (UE) 2016/680, selon le cas. Cette obligation ne s'applique pas aux systèmes d'IA utilisés pour la catégorisation biométrique et la reconnaissance des émotions dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales ou d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers et conformément au droit de l'Union.

4. Les déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage indiquent que les contenus ont été générés ou manipulés par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière. Lorsque le contenu fait partie d'une œuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre.

Les déployeurs d'un système d'IA qui génère ou manipule des textes publiés dans le but d'informer le public sur des questions d'intérêt public indiquent que le texte a été généré ou manipulé par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, ou lorsque le contenu généré par l'IA a fait l'objet d'un processus d'examen humain ou de contrôle éditorial et lorsqu'une personne physique ou morale assume la responsabilité éditoriale de la publication du contenu.

5. Les informations visées aux paragraphes 1 à 4 sont fournies aux personnes physiques concernées de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition. Les informations sont conformes aux exigences applicables en matière d'accessibilité.
6. Les paragraphes 1 à 4 n'ont pas d'incidence sur les exigences et obligations énoncées au chapitre III et sont sans préjudice des autres obligations de transparence prévues par le droit de l'Union ou le droit national pour les déployeurs de systèmes d'IA.

7. Le Bureau de l'IA encourage et facilite l'élaboration de codes de bonne pratique au niveau de l'Union afin de faciliter la mise en œuvre effective des obligations relatives à la détection et à l'étiquetage des contenus générés ou manipulés par une IA. La Commission peut adopter des actes d'exécution pour approuver ces codes de bonne pratique conformément à la procédure prévue à l'article 56, paragraphe 6. Si elle estime que le code n'est pas approprié, la Commission peut adopter un acte d'exécution précisant des règles communes pour la mise en œuvre de ces obligations conformément à la procédure d'examen prévue à l'article 98, paragraphe 2.

Chapitre V

Modèles d'IA à usage général

SECTION 1

REGLES DE CLASSIFICATION

Article 51

Classification de modèles d'IA à usage général en tant que modèles d'IA à usage général présentant un risque systémique

1. Un modèle d'IA à usage général est classé comme modèle d'IA à usage général présentant un risque systémique s'il remplit l'une des conditions suivantes:
 - a) il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence;

- b) sur la base d'une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique, il possède des capacités ou un impact équivalents à ceux énoncés au point a), compte tenu des critères définis à l'annexe XIII.
2. Un modèle d'IA à usage général est présumé avoir des capacités à fort impact conformément au paragraphe 1, point a), lorsque la quantité cumulée de calcul utilisée pour son entraînement mesurée en opérations en virgule flottante est supérieure à 1025.
3. La Commission adopte des actes délégués conformément à l'article 97 pour modifier les seuils énumérés aux paragraphes 1 et 2 du présent article, ainsi que pour compléter les critères de référence et les indicateurs à la lumière des évolutions technologiques, telles que les améliorations algorithmiques ou l'efficacité accrue du matériel informatique, si nécessaire, afin que ces seuils reflètent l'état de la technique.

Article 52

Procédure

1. Lorsqu'un modèle d'IA à usage général remplit la condition visée à l'article 51, paragraphe 1, point a), le fournisseur concerné en informe la Commission sans tarder et, en tout état de cause, dans un délai de deux semaines après la date à laquelle ce critère est rempli ou après qu'il a été établi qu'il le sera. Cette notification comprend les informations nécessaires pour démontrer que le critère pertinent a été rempli. Si la Commission apprend l'existence d'un modèle d'IA à usage général présentant un risque systémique dont elle n'a pas été informée, elle peut décider de le désigner comme modèle présentant un risque systémique.

2. Le fournisseur d'un modèle d'IA à usage général qui remplit la condition visée à l'article 51, paragraphe 1, point a), peut présenter, avec sa notification, des arguments suffisamment étayés pour démontrer que, exceptionnellement, bien qu'il remplisse ce critère, le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique et ne devrait donc pas être classé comme modèle d'IA à usage général présentant un risque systémique.
3. Lorsque la Commission conclut que les arguments présentés conformément au paragraphe 2 ne sont pas suffisamment étayés et que le fournisseur concerné n'a pas été en mesure de démontrer que le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique, elle rejette ces arguments, et le modèle d'IA à usage général est considéré comme un modèle d'IA à usage général présentant un risque systémique.
4. La Commission peut désigner un modèle d'IA à usage général comme présentant un risque systémique, d'office ou à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a), sur la base des critères énoncés à l'annexe XIII.

La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe XIII en précisant et mettant à jour les critères énoncés à ladite annexe.

5. Sur demande motivée d'un fournisseur dont le modèle a été désigné comme modèle d'IA à usage général présentant un risque systémique en vertu du paragraphe 4, la Commission tient compte de la demande et peut décider de réévaluer si le modèle d'IA à usage général peut encore être considéré comme présentant un risque systémique sur la base des critères énoncés à l'annexe XIII. Une telle demande contient les éléments objectifs, détaillés et nouveaux qui sont apparus depuis la décision de désignation. Les fournisseurs peuvent demander une réévaluation au plus tôt six mois après la décision de désignation. Lorsque la Commission, à la suite de sa réévaluation, décide de maintenir la désignation en tant que modèle d'IA à usage général présentant un risque systémique, les fournisseurs peuvent demander une réévaluation au plus tôt six mois après cette décision.
6. La Commission veille à ce qu'une liste des modèles d'IA à usage général présentant un risque systémique soit publiée et tient cette liste à jour, sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national.

SECTION 2
OBLIGATIONS INCOMBANT AUX FOURNISSEURS
DE MODELES D'IA A USAGE GENERAL

Article 53

Obligations incombant aux fournisseurs de modèles d'IA à usage général

1. Les fournisseurs de modèles d'IA à usage général:
 - a) élaborent et tiennent à jour la documentation technique du modèle, y compris son processus d'entraînement et d'essai et les résultats de son évaluation, qui contient, au minimum, les informations énoncées à l'annexe XI aux fins de la fournir, sur demande, au Bureau de l'IA et aux autorités nationales compétentes;
 - b) élaborent, tiennent à jour et mettent à disposition des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA. Sans préjudice de la nécessité d'observer et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national, ces informations et cette documentation:
 - i) permettent aux fournisseurs de systèmes d'IA d'avoir une bonne compréhension des capacités et des limites du modèle d'IA à usage général et de se conformer aux obligations qui leur incombent en vertu du présent règlement; et
 - ii) contiennent, au minimum, les éléments énoncés à l'annexe XII;

- c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790;
 - d) élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA.
2. Les obligations énoncées au paragraphe 1, points a) et b), ne s'appliquent pas aux fournisseurs de modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. Cette exception ne s'applique pas aux modèles d'IA à usage général présentant un risque systémique.
3. Les fournisseurs de modèles d'IA à usage général coopèrent, en tant que de besoin, avec la Commission et les autorités nationales compétentes dans l'exercice de leurs compétences et pouvoirs en vertu du présent règlement.

4. Les fournisseurs de modèles d'IA à usage général peuvent s'appuyer sur des codes de bonne pratique au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Le respect des normes européennes harmonisées confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations. Les fournisseurs de modèles d'IA à usage général qui n'adhèrent pas à un code de bonnes pratiques approuvé ou ne respectent pas une norme européenne harmonisée démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'appréciation de la Commission.
5. Afin de faciliter le respect de l'annexe XI, et notamment du point 2, points d) et e), la Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour préciser les méthodes de mesure et de calcul en vue de permettre l'élaboration d'une documentation comparable et vérifiable.
6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97, paragraphe 2, pour modifier les annexes XI et XII à la lumière des évolutions technologiques.
7. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

Article 54

Mandataires des fournisseurs de modèles d'IA à usage général

1. Avant de mettre un modèle d'IA à usage général sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le fournisseur autorise son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.
3. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Il fournit une copie du mandat au Bureau de l'IA à la demande de ce dernier, dans l'une des langues officielles des institutions de l'Union. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter les tâches suivantes:
 - a) vérifier que la documentation technique prévue à l'annexe XI a été rédigée et que toutes les obligations visées à l'article 53 et, le cas échéant, à l'article 55 ont été remplies par le fournisseur;
 - b) tenir à la disposition du Bureau de l'IA et des autorités nationales compétentes une copie de la documentation technique prévue à l'annexe XI, pendant une période de dix ans après la mise sur le marché du modèle d'IA à usage général, et les coordonnées du fournisseur ayant désigné le mandataire;
 - c) communiquer au Bureau de l'IA, sur demande motivée de sa part, toutes les informations et tous les documents, y compris ceux visés au point b), nécessaires pour démontrer qu'il respecte les obligations du présent chapitre;
 - d) coopérer avec le Bureau de l'IA et les autorités compétentes, sur demande motivée de leur part, à toute mesure qu'ils prennent à l'égard d'un modèle d'IA à usage général, y compris lorsque le modèle est intégré dans des systèmes d'IA mis sur le marché ou mis en service dans l'Union.

4. Le mandat habilite le mandataire à servir d'interlocuteur, en plus ou à la place du fournisseur, au Bureau de l'IA ou aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.
5. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent en vertu du présent règlement. Dans ce cas, il informe en outre immédiatement le Bureau de l'IA de la cessation du mandat et des motifs qui la sous-tendent.
6. L'obligation énoncée au présent article ne s'applique pas aux fournisseurs de modèles d'IA à usage général qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics, à moins que les modèles d'IA à usage général présentent un risque systémique.

SECTION 3
OBLIGATIONS INCOMBANT AUX FOURNISSEURS
DE MODELES D'IA A USAGE GENERAL PRESENTANT UN RISQUE SYSTEMIQUE

Article 55

Obligations incombant aux fournisseurs
de modèles d'IA à usage général présentant un risque systémique

1. Outre les obligations énumérées aux articles 53 et 54, les fournisseurs de modèles d'IA à usage général présentant un risque systémique:
 - a) effectuent une évaluation des modèles sur la base de protocoles et d'outils normalisés reflétant l'état de la technique, y compris en réalisant et en documentant des essais contradictoires des modèles en vue d'identifier et d'atténuer les risques systémiques;
 - b) évaluent et atténuent les risques systémiques éventuels au niveau de l'Union, y compris leurs origines, qui peuvent découler du développement, de la mise sur le marché ou de l'utilisation de modèles d'IA à usage général présentant un risque systémique;
 - c) suivent, documentent et communiquent sans retard injustifié au Bureau de l'IA et, le cas échéant, aux autorités nationales compétentes les informations pertinentes concernant les incidents graves ainsi que les éventuelles mesures correctives pour y remédier;
 - d) garantissent un niveau approprié de protection en matière de cybersécurité pour le modèle d'IA à usage général présentant un risque systémique et l'infrastructure physique du modèle.

2. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique peuvent s'appuyer sur des codes de bonne pratique au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Le respect des normes européennes harmonisées confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique qui n'adhèrent pas à un code de bonnes pratiques approuvé ou ne respectent pas une norme européenne harmonisée démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'appréciation de la Commission.
3. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

SECTION 4

CODES DE BONNES PRATIQUES

Article 56

Codes de bonne pratique

1. Le Bureau de l'IA encourage et facilite l'élaboration de codes de bonne pratique au niveau de l'Union afin de contribuer à la bonne application du présent règlement, en tenant compte des approches internationales.

2. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique couvrent au moins les obligations prévues aux articles 53 et 55, y compris les questions suivantes:
- a) les moyens de s'assurer que les informations visées à l'article 53, paragraphe 1, points a) et b), sont mises à jour à la lumière des évolutions du marché et des technologies;
 - b) le niveau approprié de détail pour le résumé du contenu utilisé pour l'entraînement;
 - c) l'identification du type et de la nature des risques systémiques au niveau de l'Union, y compris leurs origines, le cas échéant;
 - d) les mesures, procédures et modalités d'évaluation et de gestion des risques systémiques au niveau de l'Union, y compris la documentation y afférente, qui sont proportionnées aux risques, prennent en considération leur gravité et leur probabilité et tiennent compte des défis spécifiques que pose la maîtrise de ces risques à la lumière des différentes façons dont ils peuvent apparaître ou se concrétiser tout au long de la chaîne de valeur de l'IA.
3. Le Bureau de l'IA peut inviter tous les fournisseurs de modèles d'IA à usage général, ainsi que les autorités nationales compétentes concernées, à participer à l'élaboration de codes de bonne pratique. Les organisations de la société civile, l'industrie, le monde universitaire et d'autres parties prenantes concernées, telles que les fournisseurs en aval et les experts indépendants, peuvent apporter leur soutien au processus.

4. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique définissent clairement leurs objectifs spécifiques et contiennent des engagements ou des mesures, y compris, le cas échéant, des indicateurs de performance clés, afin de garantir la réalisation de ces objectifs, et à ce qu'ils tiennent dûment compte des besoins et des intérêts de l'ensemble des parties intéressées, y compris les personnes concernées, au niveau de l'Union.
5. Le Bureau de l'IA veille à ce que les participants aux codes de bonne pratique fassent régulièrement rapport au Bureau de l'IA sur la mise en œuvre des engagements ainsi que sur les mesures qu'ils adoptent et leurs résultats, y compris mesurés par rapport aux indicateurs de performance clés, le cas échéant. Les indicateurs de performance clés et l'obligation de présenter des rapports reflètent les différences de taille et de capacité entre les différents participants.
6. Le Bureau de l'IA et le Comité IA contrôlent et évaluent régulièrement la réalisation des objectifs des codes de bonne pratique par les participants et leur contribution à la bonne application du présent règlement. Le Bureau de l'IA et le Comité IA évaluent si les codes de bonne pratique couvrent les obligations prévues aux articles 53 et 55, et contrôlent et évaluent régulièrement la réalisation de leurs objectifs. Ils publient leur évaluation de l'adéquation des codes de bonne pratique.

La Commission peut, au moyen d'un acte d'exécution, approuver un code de bonnes pratiques et lui conférer une validité générale au sein de l'Union. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

7. Le Bureau de l'IA peut inviter tous les fournisseurs de modèles d'IA à usage général à adhérer aux codes de bonne pratique. Pour les fournisseurs de modèles d'IA à usage général ne présentant pas de risque systémique, cette adhésion peut se limiter aux obligations prévues à l'article 53, à moins qu'ils ne déclarent explicitement leur intérêt à respecter le code complet.
8. Le Bureau de l'IA encourage et facilite également, le cas échéant, le réexamen et l'adaptation des codes de bonne pratique, en particulier à la lumière des normes émergentes. Le Bureau de l'IA participe à l'évaluation des normes disponibles.
9. Les codes de bonne pratique sont prêts au plus tard le ... [*neuf mois à compter de la date d'entrée en vigueur du présent règlement*]. Le Bureau de l'IA prend les mesures nécessaires, y compris inviter les fournisseurs en vertu du paragraphe 7.

Si, à la date du ... [*douze mois à compter de la date d'entrée en vigueur du présent règlement*], un code de bonnes pratiques n'a pas pu être mis au point, ou si le Bureau de l'IA estime qu'il n'est pas approprié à la suite de son évaluation au titre du paragraphe 6 du présent article, la Commission peut prévoir, au moyen d'actes d'exécution, des règles communes pour la mise en œuvre des obligations prévues aux articles 53 et 55, y compris les questions énoncées au paragraphe 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Chapitre VI

Mesures de soutien à l'innovation

Article 57

Bacs à sable réglementaires de l'IA

1. Les États membres veillent à ce que leurs autorités compétentes mettent en place au moins un bac à sable réglementaire de l'IA au niveau national, qui est opérationnel au plus tard le ... [24 mois à compter de la date d'entrée en vigueur du présent règlement]. Ce bac à sable peut également être établi conjointement avec les autorités compétentes d'autres États membres. La Commission peut fournir un soutien technique, des conseils et des outils pour la mise en place et l'exploitation de bacs à sable réglementaires de l'IA.

L'obligation visée au premier alinéa peut également être remplie en participant à un bac à sable existant, pour autant que cette participation offre un niveau de couverture nationale équivalent pour les États membres participants.

2. Des bacs à sable réglementaires de l'IA supplémentaires au niveau régional ou au niveau local, ou établis conjointement avec les autorités compétentes d'autres États membres peuvent également être mis en place.
3. Le Contrôleur européen de la protection des données peut également créer un bac à sable réglementaire de l'IA pour les institutions, organes et organismes de l'Union, et peut exercer les rôles et les tâches des autorités nationales compétentes conformément au présent chapitre.

4. Les États membres veillent à ce que les autorités compétentes visées aux paragraphes 1 et 2 allouent des ressources suffisantes pour se conformer au présent article de manière efficace et en temps utile. Lorsqu'il y a lieu, les autorités nationales compétentes coopèrent avec d'autres autorités concernées et peuvent permettre la participation d'autres acteurs de l'écosystème de l'IA. Le présent article n'a pas d'incidence sur d'autres bacs à sable réglementaires établis en vertu du droit de l'Union ou du droit national. Les États membres assurent un niveau approprié de coopération entre les autorités chargées de la surveillance de ces autres bacs à sable et les autorités nationales compétentes.
5. Les bacs à sable réglementaires de l'IA établis en vertu du paragraphe 1 offrent un environnement contrôlé qui favorise l'innovation et facilite le développement, l'entraînement, la mise à l'essai et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique de bac à sable convenu entre les fournisseurs ou fournisseurs potentiels et l'autorité compétente. Ces bacs à sable peuvent comprendre des essais en conditions réelles qui y sont supervisés.
6. Les autorités compétentes fournissent, s'il y a lieu, des orientations, une surveillance et un soutien dans le cadre du bac à sable réglementaire de l'IA en ce qui concerne l'identification des risques, en particulier pour les droits fondamentaux, la santé et la sécurité, les essais, les mesures d'atténuation et leur efficacité par rapport aux obligations et exigences du présent règlement et, le cas échéant, d'autres dispositions du droit de l'Union et du droit national dont le respect est suivi dans le cadre du bac à sable.
7. Les autorités compétentes donnent aux fournisseurs et aux fournisseurs potentiels participant au bac à sable réglementaire de l'IA des orientations sur les attentes réglementaires et la manière de satisfaire aux exigences et obligations énoncées dans le présent règlement.

À la demande du fournisseur ou du fournisseur potentiel du système d'IA, l'autorité compétente fournit une preuve écrite des activités menées avec succès dans le bac à sable. L'autorité compétente fournit également un rapport de sortie détaillant les activités menées dans le bac à sable ainsi que les résultats et acquis d'apprentissage correspondants. Les fournisseurs peuvent utiliser ces documents pour démontrer leur conformité avec le présent règlement au moyen de la procédure d'évaluation de la conformité ou d'activités pertinentes de surveillance du marché. À cet égard, les rapports de sortie et la preuve écrite fournie par l'autorité nationale compétente sont évalués de manière positive par les autorités de surveillance du marché et les organismes notifiés, en vue d'accélérer les procédures d'évaluation de la conformité dans une mesure raisonnable.

8. Sous réserve des dispositions relatives à la confidentialité énoncées à l'article 78 et avec l'accord du fournisseur ou du fournisseur potentiel, la Commission et le Comité IA sont autorisés à accéder aux rapports de sortie et en tiennent compte, le cas échéant, dans l'exercice des tâches qui leur incombent en vertu du présent règlement. Si le fournisseur ou le fournisseur potentiel et l'autorité nationale compétente y consentent explicitement, le rapport de sortie peut être mis à la disposition du public par l'intermédiaire de la plateforme d'information unique visée au présent article.
9. La mise en place de bacs à sable réglementaires de l'IA vise à contribuer aux objectifs suivants:
 - a) améliorer la sécurité juridique afin d'assurer le respect réglementaire du présent règlement ou, le cas échéant, d'autres dispositions applicables du droit de l'Union et du droit national;
 - b) soutenir le partage des bonnes pratiques par la coopération avec les autorités participant au bac à sable réglementaire de l'IA;

- c) favoriser l'innovation et la compétitivité et faciliter la mise en place d'un écosystème d'IA;
 - d) contribuer à l'apprentissage réglementaire fondé sur des données probantes;
 - e) faciliter et accélérer l'accès au marché de l'Union pour les systèmes d'IA, en particulier lorsqu'ils sont fournis par des PME, y compris des jeunes pousses.
10. Les autorités nationales compétentes veillent à ce que, dans la mesure où les systèmes d'IA innovants impliquent le traitement de données à caractère personnel ou relèvent à d'autres titres de la surveillance d'autres autorités nationales ou autorités compétentes assurant ou encadrant l'accès aux données, les autorités nationales chargées de la protection des données et ces autres autorités nationales ou autorités compétentes soient associées à l'exploitation du bac à sable réglementaire de l'IA et participent au contrôle des aspects qui relèvent de leurs tâches et pouvoirs respectifs.
11. Les bacs à sable réglementaires de l'IA n'ont pas d'incidence sur les pouvoirs en matière de contrôle ou de mesures correctives des autorités compétentes chargées de la surveillance des bacs à sable, y compris au niveau régional ou local. Tout risque substantiel pour la santé, la sécurité et les droits fondamentaux constaté lors du développement et des tests de ces systèmes d'IA donne lieu à des mesures d'atténuation appropriées. Les autorités nationales compétentes sont habilitées à suspendre temporairement ou définitivement le processus d'essai ou la participation au bac à sable si aucune atténuation efficace n'est possible, et elles informent le Bureau de l'IA de cette décision. Les autorités nationales compétentes exercent leurs pouvoirs de surveillance, dans les limites de la législation applicable, en faisant usage de leurs pouvoirs discrétionnaires lorsqu'elles mettent en œuvre des dispositions juridiques relatives à un projet spécifique de bac à sable réglementaire de l'IA, dans le but de soutenir l'innovation dans le domaine de l'IA au sein de l'Union.

12. Les fournisseurs et les fournisseurs potentiels participant au bac à sable réglementaire de l'IA demeurent responsables, en vertu du droit de l'Union et du droit national applicable en matière de responsabilité, de tout préjudice infligé à des tiers en raison de l'expérimentation menée dans le bac à sable. Toutefois, sous réserve du respect par les fournisseurs potentiels du plan spécifique ainsi que des modalités de leur participation et de leur disposition à suivre de bonne foi les orientations fournies par l'autorité nationale compétente, aucune amende administrative n'est infligée par les autorités en cas de violation du présent règlement. Lorsque d'autres autorités compétentes chargées d'autres dispositions du droit de l'Union et du droit national ont participé activement à la surveillance du système d'IA dans le bac à sable et ont fourni des orientations en matière de conformité, aucune amende administrative n'est infligée en ce qui concerne ces dispositions.
13. Les bacs à sable réglementaires de l'IA sont conçus et mis en œuvre de manière à faciliter, le cas échéant, la coopération transfrontière entre les autorités nationales compétentes.
14. Les autorités nationales compétentes coordonnent leurs activités et coopèrent dans le cadre du Comité IA.
15. Les autorités nationales compétentes informent le Bureau de l'IA et le Comité IA de la mise en place d'un bac à sable et peuvent leur demander un soutien et des orientations. Le Bureau de l'IA publie une liste des bacs à sable prévus et existants et la tient à jour afin d'encourager une plus grande interaction dans les bacs à sable réglementaires de l'IA et la coopération transfrontière.

16. Les autorités nationales compétentes présentent des rapports annuels au Bureau de l'IA et au Comité IA, dont le premier est élaboré dans un délai d'un an à compter de la mise en place du bac à sable réglementaire de l'IA, puis tous les ans jusqu'à son terme, et un rapport final. Ces rapports fournissent des informations sur les progrès et les résultats de la mise en œuvre de ces bacs à sable, y compris les bonnes pratiques, les incidents, les enseignements et les recommandations concernant leur mise en place et, le cas échéant, sur l'application et la révision éventuelle du présent règlement, y compris ses actes délégués et actes d'exécution, et sur l'application d'autres dispositions législatives de l'Union contrôlés par les autorités compétentes dans le cadre du bac à sable. Les autorités nationales compétentes publient ces rapports annuels ou des résumés de ceux-ci en ligne. La Commission tient compte, s'il y a lieu, des rapports annuels dans l'exercice de ses tâches au titre du présent règlement.
17. La Commission développe une interface unique et spécifique contenant toutes les informations pertinentes relatives aux bacs à sable réglementaires de l'IA pour permettre aux parties prenantes d'interagir avec les bacs à sable réglementaires de l'IA et de s'informer auprès des autorités compétentes, ainsi que de demander des orientations non contraignantes sur la conformité de produits, services et modèles commerciaux innovants intégrant les technologies de l'IA, conformément à l'article 62, paragraphe 1, point c). La Commission assure une coordination proactive avec les autorités nationales compétentes, le cas échéant.

Article 58

Modalités détaillées pour les bacs à sable réglementaires de l'IA et fonctionnement de ceux-ci

1. Afin d'éviter une fragmentation à travers l'Union, la Commission adopte des actes d'exécution précisant les modalités détaillées de mise en place, de développement, de mise en œuvre, d'exploitation et de surveillance des bacs à sable réglementaires de l'IA. Les actes d'exécution contiennent des principes communs sur les questions suivantes:
 - a) les critères d'éligibilité et de sélection pour la participation au bac à sable réglementaire de l'IA;
 - b) les procédures de demande, de surveillance, de sortie et d'expiration du bac à sable réglementaire de l'IA, ainsi que de participation à celui-ci, y compris le plan du bac à sable et le rapport de sortie;
 - c) les conditions applicables aux participants.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Les actes d'exécution visés au paragraphe 1 garantissent que:
 - a) les bacs à sable réglementaires de l'IA sont ouverts à tout fournisseur ou fournisseur potentiel d'un système d'IA qui remplit les critères d'éligibilité et de sélection, lesquels sont transparents et équitables, et que les autorités nationales compétentes informent les demandeurs de leur décision dans un délai de trois mois à compter de la demande;

- b) que les bacs à sable réglementaires de l'IA permettent un accès étendu et égal et suivent la demande de participation; les fournisseurs et fournisseurs potentiels peuvent également soumettre des demandes en partenariat avec des déployeurs et d'autre tiers concernés;
- c) que les modalités détaillées pour les bacs à sable réglementaires de l'IA et les conditions relatives à ces derniers favorisent, dans toute la mesure du possible, la flexibilité permettant aux autorités nationales compétentes de mettre en place et d'exploiter leurs bacs à sable réglementaires de l'IA;
- d) que l'accès aux bacs à sable réglementaires de l'IA est gratuit pour les PME, y compris les jeunes pousses, sans préjudice des coûts exceptionnels que les autorités nationales compétentes peuvent recouvrer de manière équitable et proportionnée;
- e) qu'ils aident les fournisseurs et les fournisseurs potentiels, au moyen des acquis d'apprentissage des bacs à sable réglementaires de l'IA, à se conformer aux obligations d'évaluation de la conformité prévues par le présent règlement et à l'application volontaire des codes de conduite visés à l'article 95;
- f) que les bacs à sable réglementaires de l'IA facilitent la participation d'autres acteurs pertinents au sein de l'écosystème de l'IA, tels que les organismes notifiés et les organisations de normalisation, les PME, y compris les jeunes pousses, les entreprises, les innovateurs, les installations d'expérimentation et d'essai, les laboratoires de recherche et d'expérimentation et les pôles européens d'innovation numérique, les centres d'excellence, les chercheurs individuels, afin de permettre et de faciliter la coopération avec les secteurs public et privé;

- g) que les procédures, processus et exigences administratives applicables en matière de demande, de sélection, de participation et de sortie dans le cadre du bac à sable réglementaires de l'IA sont simples, facilement compréhensibles et clairement communiqués afin de faciliter la participation des PME, y compris des jeunes pousses, disposant de capacités juridiques et administratives limitées, et sont rationalisés dans toute l'Union, afin d'éviter la fragmentation et de permettre que la participation à un bac à sable réglementaire de l'IA mis en place par un État membre ou par le Contrôleur européen de la protection des données soit mutuellement et uniformément reconnue et produise les mêmes effets juridiques dans l'ensemble de l'Union;
 - h) que la participation au bac à sable réglementaire de l'IA est limitée à une période adaptée à la complexité et à l'envergure du projet, qui peut être prolongée par l'autorité nationale compétente;
 - i) que les bacs à sable réglementaire de l'IA facilitent le développement d'outils et d'infrastructures pour la mise à l'essai, l'étalonnage des performances, l'évaluation et l'explication des aspects des systèmes d'IA pertinents pour l'apprentissage réglementaire, tels que la précision, la solidité et la cybersécurité, ainsi que les mesures d'atténuation des risques d'atteinte aux droits fondamentaux et à la société au sens large.
3. Les fournisseurs potentiels dans les bacs à sable réglementaires de l'IA, en particulier les PME et les jeunes pousses, sont dirigés, le cas échéant, vers des services préalables au déploiement, tels que des orientations sur la mise en œuvre du présent règlement, et vers d'autres services à valeur ajoutée, tels que l'aide avec les documents de normalisation et la certification, les installations d'essai et d'expérimentation, les pôles européens d'innovation numérique et les centres d'excellence.

4. Lorsque les autorités nationales compétentes envisagent d'autoriser des essais en conditions réelles supervisés dans le cadre d'un bac à sable réglementaire de l'IA établi en vertu du présent article, elles conviennent spécifiquement des conditions de ces essais et, en particulier, des garanties appropriées avec les participants en vue de protéger les droits fondamentaux, la santé et la sécurité. Le cas échéant, elles coopèrent avec d'autres autorités nationales compétentes en vue d'assurer la cohérence des pratiques dans l'ensemble de l'Union.

Article 59

Traitement ultérieur de données à caractère personnel en vue du développement de certains systèmes d'IA dans l'intérêt public dans le cadre du bac à sable réglementaire de l'IA

1. Dans le bac à sable réglementaire de l'IA, les données à caractère personnel collectées légalement à d'autres fins peuvent être traitées uniquement aux fins du développement, de l'entraînement et de la mise à l'essai de certains systèmes d'IA dans le bac à sable, lorsque l'ensemble des conditions suivantes sont remplies:
 - a) les systèmes d'IA sont développés pour préserver des intérêts publics importants par une autorité publique ou une autre personne physique ou morale et dans un ou plusieurs des domaines suivants:
 - i) la sécurité publique et la santé publique, y compris la détection, le diagnostic, la prévention, le contrôle et le traitement des maladies ainsi que l'amélioration des systèmes de soins de santé;
 - ii) un niveau élevé de protection et d'amélioration de la qualité de l'environnement, la protection de la biodiversité, la protection contre la pollution, les mesures de transition écologique et les mesures d'atténuation du changement climatique et d'adaptation à celui-ci;

- iii) la durabilité énergétique;
 - iv) la sécurité et la résilience des systèmes de transport et de la mobilité, des infrastructures critiques et des réseaux de transport;
 - v) l'efficacité et la qualité de l'administration publique et des services publics;
- b) les données traitées sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au chapitre III, section 2, lorsque ces exigences ne peuvent être satisfaites de manière efficace en traitant des données anonymisées, synthétiques ou autres à caractère non personnel;
- c) il existe des mécanismes de suivi efficaces pour déterminer si des risques élevés pour les droits et les libertés des personnes concernées, visés à l'article 35 du règlement (UE) 2016/679 et à l'article 39 du règlement (UE) 2018/1725, sont susceptibles de survenir lors de l'expérimentation menée dans le cadre du bac à sable, ainsi que des mécanismes de réponse permettant d'atténuer rapidement ces risques et, au besoin, de faire cesser le traitement des données;
- d) les données à caractère personnel à traiter dans le cadre du bac à sable se trouvent dans un environnement de traitement des données séparé, isolé et protégé sur le plan fonctionnel, placé sous le contrôle du fournisseur potentiel, et seules les personnes autorisées ont accès à ces données;
- e) les fournisseurs ne peuvent en outre partager les données initialement collectées que conformément au droit de l'Union en matière de protection des données; aucune donnée à caractère personnel créée dans le bac à sable ne peut être partagée en dehors du bac à sable;

- f) aucun traitement de données à caractère personnel effectué dans le cadre du bac à sable ne débouche sur des mesures ou des décisions affectant les personnes concernées ni n'a d'incidence sur l'application des droits que leur confère le droit de l'Union en matière de protection des données à caractère personnel;
- g) les données à caractère personnel traitées dans le cadre du bac à sable sont protégées par des mesures techniques et organisationnelles appropriées et supprimées une fois que la participation au bac à sable a cessé ou que la période de conservation de ces données à caractère personnel a expiré;
- h) les registres du traitement des données à caractère personnel dans le cadre du bac à sable sont conservés pendant la durée de la participation au bac à sable, sauf disposition contraire du droit de l'Union ou du droit national;
- i) une description complète et détaillée du processus et de la justification de l'entraînement, de la mise à l'essai et de la validation du système d'IA est conservée avec les résultats des essais, et fait partie de la documentation technique visée à l'annexe IV;
- j) un résumé succinct du projet d'IA développé dans le cadre du bac à sable, de ses objectifs et des résultats escomptés est publié sur le site web des autorités compétentes; cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

2. Aux fins de la prévention et de la détection d'infractions pénales, ainsi que des enquêtes et des poursuites en la matière ou de l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, sous le contrôle et la responsabilité des autorités répressives, le traitement des données à caractère personnel dans les bacs à sable réglementaires de l'IA est fondé sur une disposition spécifique du droit de l'Union ou du droit national et soumis aux mêmes conditions cumulatives que celles visées au paragraphe 1.
3. Le paragraphe 1 est sans préjudice du droit de l'Union ou du droit national excluant le traitement des données à caractère personnel à des fins autres que celles expressément mentionnées dans ce droit, ainsi que sans préjudice du droit de l'Union ou du droit national établissant le fondement du traitement des données à caractère personnel qui est nécessaire aux fins du développement, de la mise à l'essai et de l'entraînement de systèmes d'IA innovants, ou de toute autre base juridique, dans le respect du droit de l'Union relatif à la protection des données à caractère personnel.

Article 60

Essais de systèmes d'IA à haut risque en conditions réelles en dehors des bacs à sable réglementaires de l'IA

1. Les essais de systèmes d'IA à haut risque en conditions réelles en dehors des bacs à sable réglementaires de l'IA peuvent être effectués par les fournisseurs ou fournisseurs potentiels de systèmes d'IA à haut risque énumérés à l'annexe III, conformément au présent article et au plan d'essais en conditions réelles visé au présent article, sans préjudice des interdictions prévues à l'article 5.

La Commission précise, par voie d'actes d'exécution, les éléments détaillés du plan d'essais en conditions réelles. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Le présent paragraphe est sans préjudice du droit de l'Union ou du droit national relatif aux essais en conditions réelles de systèmes d'IA à haut risque liés aux produits qui relèvent de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.

2. Les fournisseurs ou fournisseurs potentiels peuvent effectuer, seuls ou en partenariat avec un ou plusieurs déployeurs ou déployeurs potentiels, des essais des systèmes d'IA à haut risque visés à l'annexe III, en conditions réelles, à tout moment avant la mise sur le marché ou la mise en service du système d'IA concerné.
3. Les essais de systèmes d'IA à haut risque en conditions réelles au titre du présent article sont sans préjudice de tout examen éthique exigé par le droit de l'Union ou le droit national.
4. Les fournisseurs ou fournisseurs potentiels ne peuvent effectuer les essais en conditions réelles que si toutes les conditions suivantes sont remplies:
 - a) le fournisseur ou le fournisseur potentiel a établi un plan d'essais en conditions réelles et l'a soumis à l'autorité de surveillance du marché dans l'État membre où les essais en conditions réelles doivent être réalisés;
 - b) l'autorité de surveillance du marché de l'État membre où les essais en conditions réelles doivent être réalisés a approuvé les essais en conditions réelles et le plan d'essais en conditions réelles; lorsque l'autorité de surveillance du marché n'a pas fourni de réponse dans un délai de 30 jours, les essais en conditions réelles et le plan d'essais en conditions réelles sont réputés approuvés; lorsque le droit national ne prévoit pas d'approbation tacite, les essais en conditions réelles restent soumis à autorisation;

- c) le fournisseur ou fournisseur potentiel, à l'exception des fournisseurs ou fournisseurs potentiels de systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, ainsi que des systèmes d'IA à haut risque visés à l'annexe III, point 2, a enregistré les essais en conditions réelles dans la partie non publique de la base de données de l'UE visée à l'article 71, paragraphe 3, avec un numéro d'identification unique à l'échelle de l'Union et les informations indiquées à l'annexe IX; le fournisseur ou fournisseur potentiel de systèmes d'IA à haut risque visé à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, a enregistré les essais en conditions réelles dans la partie non publique de la base de données de l'UE visée à l'article 49, paragraphe 4, point d), avec un numéro d'identification unique à l'échelle de l'Union et les informations y indiquées; le fournisseur ou fournisseur potentiel de systèmes d'IA à haut risque visé à l'annexe III, point 2, a enregistré les essais en conditions réelles conformément à l'article 49, paragraphe 5.
- d) le fournisseur ou fournisseur potentiel effectuant les essais en conditions réelles est établi dans l'Union ou a désigné un représentant légal établi dans l'Union;
- e) les données collectées et traitées aux fins des essais en conditions réelles ne sont transférées vers des pays tiers qu'à condition que des garanties appropriées et applicables en vertu du droit de l'Union soient en place;

- f) les essais en conditions réelles ne durent pas plus longtemps que nécessaire pour atteindre leurs objectifs et, en tout état de cause, pas plus de six mois, qui peuvent être prolongés pour une période supplémentaire de six mois, sous réserve d'une notification préalable par le fournisseur ou fournisseur potentiel à l'autorité de surveillance du marché, accompagnée d'une explication des raisons qui motivent une telle prolongation;
- g) les participants aux essais en conditions réelles qui sont des personnes appartenant à des groupes vulnérables en raison de leur âge ou de leur handicap sont dûment protégées;
- h) lorsqu'un fournisseur ou un fournisseur potentiel organise les essais en conditions réelles en coopération avec un ou plusieurs déployeurs ou déployeurs potentiels, ces derniers ont été préalablement informés de tous les aspects des essais qui sont pertinents pour leur décision de participer et ont reçu les instructions d'utilisation adéquates pour le système d'IA visé à l'article 13; le fournisseur ou fournisseur potentiel et le déployeur ou déployeur potentiel concluent un accord précisant leurs rôles et responsabilités en vue d'assurer le respect des dispositions relatives aux essais en conditions réelles prévues par le présent règlement et en vertu d'autres dispositions applicables du droit de l'Union et du droit national;
- i) les participants aux essais en conditions réelles ont donné leur consentement éclairé conformément à l'article 61 ou, dans le cas des services répressifs, lorsque la recherche d'un consentement éclairé empêcherait de réaliser les essais du système d'IA, les essais proprement dits et les résultats des essais en conditions réelles n'ont pas d'effet négatif sur les participants, et leurs données à caractère personnel sont supprimées une fois les essais réalisés;

- j) le fournisseur ou le fournisseur potentiel ainsi que les déployeurs ou les déployeurs potentiels effectuent un contrôle effectif des essais en conditions réelles, par des personnes dûment qualifiées dans le domaine concerné et disposant des capacités, de la formation et de l'autorité nécessaires pour accomplir leurs tâches;
 - k) les prévisions, recommandations ou décisions du système d'IA peuvent effectivement être infirmées et ignorées.
5. Tout participant aux essais en conditions réelles, ou son représentant légal, selon le cas, peut, sans encourir de préjudice et sans devoir se justifier, se retirer des essais à tout moment, en révoquant son consentement éclairé et peut demander la suppression immédiate et définitive de ses données à caractère personnel. Le retrait du consentement éclairé n'affecte pas les activités déjà menées.
6. Conformément à l'article 75, les États membres confèrent à leurs autorités de surveillance du marché le pouvoir d'exiger des fournisseurs et des fournisseurs potentiels qu'ils fournissent des informations, de procéder à des inspections inopinées à distance ou sur place et d'effectuer des vérifications concernant la réalisation des essais en conditions réelles et des systèmes d'IA à haut risque connexes. Les autorités de surveillance du marché utilisent ces pouvoirs pour veiller au développement sûr des essais en conditions réelles.

7. Tout incident grave constaté au cours des essais en conditions réelles est signalé à l'autorité nationale de surveillance du marché, conformément à l'article 73. Le fournisseur ou fournisseur potentiel adopte des mesures d'atténuation immédiates ou, à défaut, suspend les essais en conditions réelles jusqu'à ce que cette atténuation soit effective ou y met fin en l'absence d'atténuation. Le fournisseur ou fournisseur potentiel établit une procédure pour le rappel rapide du système d'IA lors de la cessation des essais en conditions réelles.
8. Les fournisseurs ou fournisseurs potentiels informent l'autorité nationale de surveillance du marché de l'État membre où les essais en conditions réelles doivent être réalisés de la suspension ou de la cessation des essais en conditions réelles et des résultats finaux.
9. Le fournisseur ou le fournisseur potentiel sont responsables, en vertu du droit de l'Union et du droit national applicable en matière de responsabilité, de tout préjudice causé durant les essais en conditions réelles.

Article 61

Consentement éclairé à participer aux essais en conditions réelles en dehors des bacs à sable réglementaires de l'IA

1. Aux fins des essais en conditions réelles visés à l'article 60, le consentement éclairé donné librement est obtenu des participants aux essais avant que ceux-ci ne prennent part à ces essais et après qu'ils ont été dûment informés au moyen d'informations concises, claires, pertinentes et compréhensibles concernant:
 - a) la nature et les objectifs des essais en conditions réelles ainsi que les désagréments éventuels pouvant être liés à sa participation;
 - b) les conditions dans lesquelles les essais en conditions réelles doivent être réalisés, y compris la durée prévue de la participation;
 - c) les droits et garanties concernant leur participation, en particulier leur droit de refuser de participer aux essais en conditions réelles et leur droit de s'en retirer à tout moment sans encourir de préjudice et sans devoir se justifier;
 - d) les modalités selon lesquelles il peut être demandé que des prévisions, recommandations ou décisions du système d'IA soient infirmées ou ignorées;
 - e) le numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles conformément à l'article 60, paragraphe 4, point c), et les coordonnées du fournisseur ou de son représentant légal auprès duquel des informations complémentaires peuvent être obtenues.

2. Le consentement éclairé est daté et documenté et une copie en est remise aux participants aux essais ou à leur représentant légal.

Article 62

Mesures en faveur des fournisseurs et déployeurs, en particulier les PME, y compris les jeunes pousses

1. Les États membres:
 - a) accordent aux PME, y compris les jeunes pousses, qui ont leur siège social ou une succursale dans l'Union, un accès prioritaire aux bacs à sable réglementaires de l'IA, dans la mesure où elles remplissent les conditions d'éligibilité et les critères de sélection; l'accès prioritaire n'empêche pas d'autres PME, y compris les jeunes pousses, autres que celles visées au présent alinéa, d'accéder au bac à sable réglementaire de l'IA, pour autant qu'elles remplissent également les conditions d'éligibilité et les critères de sélection;
 - b) organisent des activités spécifiques de sensibilisation et de formation à l'application du présent règlement, adaptées aux besoins des PME, y compris les jeunes pousses, les déployeurs et, si nécessaire, les pouvoirs publics locaux;
 - c) utilisent des canaux privilégiés existants et, s'il y a lieu, en établissent de nouveaux avec les PME, y compris les jeunes pousses, les déployeurs, d'autres innovateurs et, si nécessaire, les pouvoirs publics locaux, afin de fournir des conseils et de répondre aux questions relatives à la mise en œuvre du présent règlement, y compris en ce qui concerne la participation à des bacs à sable réglementaires de l'IA;

- d) facilitent la participation des PME et d'autres parties concernées au processus d'élaboration de la normalisation.
2. Les intérêts et les besoins spécifiques des PME fournisseuses, y compris les jeunes pousses, sont pris en considération lors de la fixation des frais liés à l'évaluation de la conformité visée à l'article 43, ces frais étant réduits proportionnellement à leur taille, à la taille de leur marché et à d'autres indicateurs pertinents.
3. Le Bureau de l'IA:
- a) fournit des modèles normalisés pour les domaines qui relèvent du présent règlement, comme précisé par le Comité IA dans sa demande;
 - b) met au point et tient à jour une plateforme d'information unique fournissant des informations faciles à utiliser en rapport avec le présent règlement pour tous les opérateurs dans l'ensemble de l'Union;
 - c) organise des campagnes de communication appropriées pour sensibiliser aux obligations découlant du présent règlement;
 - d) évalue et promeut la convergence des bonnes pratiques en matière de procédures de passation de marchés publics en ce qui concerne les systèmes d'IA.

Article 63

Dérogations pour des opérateurs spécifiques

1. Les microentreprises au sens de la recommandation 2003/361/CE peuvent se conformer de manière simplifiée à certains éléments du système de gestion de la qualité requis par l'article 17 du présent règlement, pour autant qu'elles n'aient pas d'entreprises partenaires ou d'entreprises liées au sens de ladite recommandation. À cette fin, la Commission élabore des lignes directrices sur les éléments du système de gestion de la qualité qui peuvent être respectés de manière simplifiée en tenant compte des besoins des microentreprises, sans affecter le niveau de protection ni la nécessité de se conformer aux exigences relatives aux systèmes d'IA à haut risque.
2. Le paragraphe 1 du présent article ne peut être interprété comme dispensant ces opérateurs de satisfaire à d'autres exigences ou obligations prévues par le présent règlement, y compris celles établies aux articles 9, 10, 11, 12, 13, 14, 15, 72 et 73.

Chapitre VII

Gouvernance

SECTION 1

GOUVERNANCE AU NIVEAU DE L'UNION

Article 64

Bureau de l'IA

1. La Commission développe l'expertise et les capacités de l'Union dans le domaine de l'IA par l'intermédiaire du Bureau de l'IA.
2. Les États membres facilitent l'accomplissement des tâches confiées au Bureau de l'IA, telles qu'elles sont définies dans le présent règlement.

Article 65

Création et structure du Comité européen de l'intelligence artificielle

1. Un Comité européen de l'intelligence artificielle (ci-après dénommé "Comité IA") est créé.

2. Le Comité IA est composé d'un représentant par État membre. Le Contrôleur européen de la protection des données participe en qualité d'observateur. Le Bureau de l'IA assiste également aux réunions du Comité IA sans toutefois prendre part aux votes. D'autres autorités, organes ou experts nationaux et de l'Union peuvent être invités aux réunions par le Comité IA au cas par cas, lorsque les questions examinées relèvent de leurs compétences.
3. Chaque représentant est désigné par son État membre pour une période de trois ans, renouvelable une fois.
4. Les États membres veillent à ce que leurs représentants au sein du Comité IA:
 - a) disposent des compétences et pouvoirs pertinents dans leur État membre afin de contribuer activement à l'accomplissement des tâches du Comité IA visées à l'article 66;
 - b) soient désignés comme point de contact unique vis-à-vis du Comité IA et, lorsqu'il y a lieu, compte tenu des besoins des États membres, comme point de contact unique pour les parties prenantes;
 - c) soient habilités à faciliter la cohérence et la coordination entre les autorités nationales compétentes de leur État membre en ce qui concerne la mise en œuvre du présent règlement, y compris par la collecte de données et d'informations pertinentes aux fins de l'accomplissement de leurs tâches au sein du Comité IA.
5. Les représentants désignés des États membres adoptent le règlement intérieur du Comité IA à la majorité des deux tiers. Le règlement intérieur établit, en particulier, les procédures de sélection, la durée du mandat et les spécifications des missions du président, les modalités de vote détaillées et l'organisation des activités du Comité IA et de celles de ses sous-groupes.

6. Le Comité IA établit deux sous-groupes permanents chargés de fournir une plateforme de coopération et d'échange entre les autorités de surveillance du marché et les autorités notifiantes au sujet des questions liées à la surveillance du marché et aux organismes notifiés respectivement.

Le sous-groupe permanent pour la surveillance du marché devrait agir au titre de groupe de coopération administrative (ADCO) pour le présent règlement au sens de l'article 30 du règlement (UE) 2019/1020.

Le Comité IA peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le cas échéant, des représentants du forum consultatif visé à l'article 67 peuvent être invités à ces sous-groupes ou à des réunions spécifiques de ces sous-groupes en qualité d'observateurs.

7. Le Comité IA est organisé et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités.
8. Le Comité IA est présidé par l'un des représentants des États membres. Le Bureau de l'IA assure le secrétariat du Comité IA, convoque les réunions à la demande du président et prépare l'ordre du jour conformément aux tâches du Comité IA au titre du présent règlement et à son règlement intérieur.

Article 66
Tâches du Comité IA

Le Comité IA conseille et assiste la Commission et les États membres afin de faciliter l'application cohérente et efficace du présent règlement. À cette fin, le Comité IA peut notamment:

- a) contribuer à la coordination entre les autorités nationales compétentes chargées de l'application du présent règlement et, en coopération avec les autorités de surveillance du marché concernées et sous réserve de leur accord, soutenir les activités conjointes des autorités de surveillance du marché visées à l'article 74, paragraphe 11;
- b) recueillir l'expertise technique et réglementaire ainsi que les bonnes pratiques et les partager entre les États membres;
- c) fournir des conseils sur la mise en œuvre du présent règlement, en particulier en ce qui concerne le contrôle de l'application des règles relatives aux modèles d'IA à usage général;
- d) contribuer à l'harmonisation des pratiques administratives dans les États membres, y compris en ce qui concerne la dérogation à la procédure d'évaluation de la conformité visée à l'article 46, le fonctionnement des bacs à sable réglementaires de l'IA et les essais en conditions réelles visés aux articles 57, 59 et 60;

- e) à la demande de la Commission ou de sa propre initiative, émettre des recommandations et des avis écrits sur toute question pertinente liée à la mise en œuvre du présent règlement et à son application cohérente et efficace, y compris:
- i) sur l'élaboration et l'application de codes de conduite et de codes de bonne pratique conformément au présent règlement, ainsi que des lignes directrices de la Commission;
 - ii) sur l'évaluation et le réexamen du présent règlement conformément à l'article 112, y compris en ce qui concerne les signalements d'incidents graves visés à l'article 73, le fonctionnement de la base de données de l'UE visée à l'article 71, l'élaboration des actes délégués ou des actes d'exécution, ainsi que les alignements éventuels du présent règlement sur les dispositions d'harmonisation de la législation de l'Union figurant à l'annexe I;
 - iii) sur les spécifications techniques ou les normes existantes se rapportant aux exigences énoncées au chapitre III, section 2;
 - iv) sur l'utilisation des normes harmonisées ou des spécifications communes visées aux articles 40 et 41;
 - v) sur les tendances, telles que la compétitivité mondiale de l'Europe dans le domaine de l'IA, l'adoption de l'IA dans l'Union et le développement des compétences numériques;
 - vi) sur les tendances concernant l'évolution de la typologie des chaînes de valeur de l'IA, en particulier en ce qui concerne les conséquences qui en découlent en termes de responsabilité;

- vii) sur la nécessité éventuelle de modifier l'annexe III conformément à l'article 7, et sur la nécessité éventuelle d'une révision de l'article 5 conformément à l'article 112, en tenant compte des éléments probants pertinents disponibles et des dernières évolutions technologiques;
- f) soutenir la Commission afin de promouvoir la maîtrise de l'IA, la sensibilisation du public et la compréhension des avantages, des risques, des garanties, des droits et des obligations liés à l'utilisation des systèmes d'IA;
- g) faciliter l'élaboration de critères communs et d'une interprétation commune, entre les opérateurs du marché et les autorités compétentes, des concepts pertinents prévus par le présent règlement, y compris en contribuant au développement de critères de référence;
- h) coopérer, lorsqu'il y a lieu, avec d'autres institutions, organes et organismes de l'Union, ainsi que des groupes d'experts et réseaux compétents de l'Union, en particulier dans les domaines de la sécurité des produits, de la cybersécurité, de la concurrence, des services numériques et des services de médias, des services financiers, de la protection des consommateurs, de la protection des données et des droits fondamentaux;
- i) contribuer à une coopération efficace avec les autorités compétentes de pays tiers et des organisations internationales;
- j) aider les autorités nationales compétentes et la Commission à développer l'expertise organisationnelle et technique nécessaire à la mise en œuvre du présent règlement, y compris en contribuant à l'évaluation des besoins de formation du personnel des États membres participant à la mise en œuvre du présent règlement;

- k) aider le Bureau de l'IA à soutenir les autorités nationales compétentes dans la mise en place et le développement de bacs à sable réglementaires de l'IA, et faciliter la coopération et le partage d'informations entre les bacs à sable réglementaires de l'IA;
- l) contribuer à l'élaboration de documents d'orientation et fournir des conseils pertinents en la matière;
- m) conseiller la Commission sur les questions internationales en matière d'IA;
- n) fournir des avis à la Commission sur les alertes qualifiées concernant les modèles d'IA à usage général;
- o) recevoir des avis des États membres sur les alertes qualifiées concernant les modèles d'IA à usage général, ainsi que sur les expériences et pratiques nationales en matière de suivi et de contrôle de l'application des systèmes d'IA, en particulier des systèmes intégrant les modèles d'IA à usage général.

Article 67

Forum consultatif

1. Un forum consultatif est créé pour fournir une expertise technique et conseiller le Comité IA et la Commission, ainsi que pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.
2. La composition du forum consultatif est équilibrée en ce qui concerne la représentation des parties prenantes, y compris l'industrie, les jeunes pousses, les PME, la société civile et le monde universitaire. La composition du forum consultatif est équilibrée sur le plan des intérêts commerciaux et non commerciaux et, dans la catégorie des intérêts commerciaux, en ce qui concerne les PME et les autres entreprises.

3. La Commission nomme les membres du forum consultatif, conformément aux critères énoncés au paragraphe 2, parmi les parties prenantes possédant une expertise reconnue dans le domaine de l'IA.
4. La durée du mandat des membres du forum consultatif est de deux ans et peut être prolongée au maximum de quatre ans.
5. L'Agence des droits fondamentaux, l'ENISA, le Comité européen de normalisation (CEN), le Comité européen de normalisation électrotechnique (CENELEC) et l'Institut européen de normalisation des télécommunications (ETSI) sont membres permanents du forum consultatif.
6. Le forum consultatif établit son règlement intérieur. Il élit parmi ses membres deux coprésidents, conformément aux critères énoncés au paragraphe 2. Leur mandat est d'une durée de deux ans, renouvelable une fois.
7. Le forum consultatif tient des réunions régulières au moins deux fois par an. Il peut inviter des experts et d'autres parties prenantes à ses réunions.
8. Le forum consultatif peut préparer des avis, des recommandations et des contributions écrites à la demande du Comité IA ou de la Commission.
9. Le forum consultatif peut créer des sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques liées aux objectifs du présent règlement.
10. Le forum consultatif prépare un rapport annuel sur ses activités. Ce rapport est rendu public.

Article 68

Groupe scientifique d'experts indépendants

1. La Commission adopte, au moyen d'un acte d'exécution, des dispositions relatives à la constitution d'un groupe scientifique d'experts indépendants (ci-après dénommé "groupe scientifique") destiné à soutenir les activités de contrôle de l'application du présent règlement. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.
2. Le groupe scientifique est composé d'experts sélectionnés par la Commission en fonction de leur expertise à la pointe des connaissances scientifiques ou techniques dans le domaine de l'IA, nécessaire pour s'acquitter des tâches énoncées au paragraphe 3, et est en mesure de démontrer qu'ils remplissent toutes les conditions suivantes:
 - a) disposer d'une expertise et d'une compétence particulières ainsi que d'une expertise scientifique ou technique dans le domaine de l'IA;
 - b) être indépendant vis-à-vis de tout fournisseur de systèmes d'IA ou de modèles d'IA à usage général;
 - c) être capable de mener des activités avec diligence, précision et objectivité.

La Commission, en consultation avec le Comité IA, détermine le nombre d'experts au sein du groupe scientifique en fonction des besoins et veille à une représentation équitable entre les hommes et les femmes ainsi que sur le plan géographique.

3. Le groupe scientifique conseille et soutient le Bureau de l'IA, notamment en ce qui concerne les tâches suivantes:
- a) soutenir la mise en œuvre et le contrôle de l'application du présent règlement en ce qui concerne les modèles et systèmes d'IA à usage général, en particulier:
 - i) en alertant le Bureau de l'IA au sujet d'éventuels risques systémiques posés au niveau de l'Union par des modèles d'IA à usage général, conformément à l'article 90;
 - ii) en contribuant à la mise au point d'outils et de méthodologies destinés à évaluer les capacités des modèles et systèmes d'IA à usage général, y compris au moyen de critères de référence;
 - iii) en fournissant des conseils quant à la classification des modèles d'IA à usage général présentant un risque systémique;
 - iv) en fournissant des conseils quant à la classification de différents modèles et systèmes d'IA à usage général;
 - v) en contribuant à la mise au point d'outils et de modèles;
 - b) soutenir, à leur demande, les autorités de surveillance du marché dans leur travail;
 - c) soutenir les activités transfrontières de surveillance du marché visées à l'article 74, paragraphe 11, sans préjudice des pouvoirs des autorités de surveillance du marché;

- d) soutenir le Bureau de l'IA dans l'exercice de ses fonctions dans le cadre de la procédure de sauvegarde de l'Union prévue à l'article 81.
4. Les experts du groupe scientifique s'acquittent de leurs tâches avec impartialité et objectivité, et garantissent la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités. Ils ne sollicitent ni n'acceptent d'instructions de quiconque dans l'exercice des tâches qui leur incombent en vertu du paragraphe 3. Chaque expert établit une déclaration d'intérêts qui est rendue publique. Le Bureau de l'IA met en place des systèmes et des procédures visant à prévenir et gérer efficacement les conflits d'intérêts potentiels.
5. L'acte d'exécution visé au paragraphe 1 comprend des dispositions sur les conditions, les procédures et les modalités détaillées permettant au groupe scientifique et à ses membres d'émettre des alertes et de demander l'assistance du Bureau de l'IA pour l'exécution des tâches du groupe scientifique.

Article 69

Accès des États membres au groupe scientifique

1. Les États membres peuvent faire appel à des experts du groupe scientifique pour soutenir leurs activités de contrôle de l'application du présent règlement.

2. Les États membres peuvent être tenus de payer des honoraires pour les conseils et le soutien fournis par les experts. La structure et le niveau des honoraires ainsi que le barème et la structure des dépens récupérables sont définis dans l'acte d'exécution visé à l'article 68, paragraphe 1, en tenant compte des objectifs consistant à mettre en œuvre le présent règlement de façon appropriée, à assurer un bon rapport coût-efficacité et à garantir que tous les États membres aient un accès effectif à des experts.
3. La Commission facilite l'accès en temps utile des États membres aux experts, en fonction des besoins, et veille à ce que la combinaison des activités de soutien menées par les structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 84 et par les experts au titre du présent article soit organisée de manière efficace et apporte la meilleure valeur ajoutée possible.

SECTION 2

AUTORITES NATIONALES COMPETENTES

Article 70

Désignation des autorités nationales compétentes et des points de contact uniques

1. Chaque État membre établit ou désigne en tant qu'autorités nationales compétentes au moins une autorité notifiante et au moins une autorité de surveillance du marché aux fins du présent règlement. Ces autorités nationales compétentes exercent leurs pouvoirs de manière indépendante, impartiale et sans parti pris, afin de préserver l'objectivité de leurs activités et de leurs tâches et d'assurer l'application et la mise en œuvre du présent règlement. Les membres de ces autorités s'abstiennent de tout acte incompatible avec leurs fonctions. Pour autant que ces principes soient respectés, les activités et tâches précitées peuvent être exécutées par une ou plusieurs autorités désignées, en fonction des besoins organisationnels de l'État membre.
2. Les États membres communiquent à la Commission les autorités notifiantes et les autorités de surveillance du marché désignées et les tâches incombant à ces autorités, ainsi que toute modification ultérieure y afférente. Les États membres rendent publiques des informations sur la manière dont les autorités compétentes et les points de contact uniques peuvent être contactés, par voie électronique, au plus tard le ... [*douze mois à compter de la date d'entrée en vigueur du présent règlement*]. Les États membres désignent une autorité de surveillance du marché pour faire office de point de contact unique pour le présent règlement et communiquent à la Commission l'identité du point de contact unique. La Commission publie une liste des points de contact uniques.

3. Les États membres veillent à ce que leurs autorités nationales compétentes disposent de ressources techniques, financières et humaines suffisantes, ainsi que d'infrastructures pour mener à bien efficacement les tâches qui leur sont confiées en vertu du présent règlement. En particulier, les autorités nationales compétentes disposent en permanence d'un personnel en nombre suffisant, qui possède, parmi ses compétences et son expertise, une compréhension approfondie des technologies de l'IA, des données et du traitement de données, de la protection des données à caractère personnel, de la cybersécurité, des droits fondamentaux, des risques pour la santé et la sécurité, et une connaissance des normes et exigences légales en vigueur. Chaque année, les États membres évaluent et, si nécessaire, mettent à jour les exigences portant sur les compétences et les ressources visées au présent paragraphe.
4. Les autorités nationales compétentes prennent des mesures appropriées pour garantir un niveau adapté de cybersécurité.
5. Dans le cadre de l'accomplissement de leurs tâches, les autorités nationales compétentes agissent conformément aux obligations de confidentialité énoncées à l'article 78.
6. Au plus tard le ... [*un an à compter de la date d'entrée en vigueur du présent règlement*], et tous les deux ans par la suite, les États membres font rapport à la Commission sur l'état des ressources financières et humaines des autorités nationales compétentes, et lui présentent une évaluation de l'adéquation de ces ressources. La Commission transmet ces informations au Comité IA pour discussion et recommandations éventuelles.
7. La Commission facilite les échanges d'expériences entre les autorités nationales compétentes.

8. Les autorités nationales compétentes peuvent fournir des orientations et des conseils sur la mise en œuvre du présent règlement, en particulier aux PME, y compris les jeunes pousses, en tenant compte des orientations et conseils du Comité IA et de la Commission, selon le cas. Chaque fois que les autorités nationales compétentes envisagent de fournir des orientations et des conseils concernant un système d'IA dans des domaines relevant d'autres actes législatifs de l'Union, les autorités compétentes nationales en vertu de ces actes législatifs de l'Union sont consultées, le cas échéant.
9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données agit en tant qu'autorité compétente responsable de leur surveillance.

Chapitre VIII

Base de données de l'UE pour les systèmes d'IA à haut risque

Article 71

Base de données de l'UE pour les systèmes d'IA à haut risque énumérés à l'annexe III

1. La Commission, en collaboration avec les États membres, crée et tient à jour une base de données de l'UE contenant les informations visées aux paragraphes 2 et 3 du présent article en ce qui concerne les systèmes d'IA à haut risque visés à l'article 6, paragraphe 2, qui sont enregistrés conformément aux articles 49 et 60 et les systèmes d'IA qui ne sont pas considérés à haut risque en vertu de l'article 6, paragraphe 3, et qui sont enregistrés conformément à l'article 6, paragraphe 4, et à l'article 49. Lorsqu'elle définit les spécifications fonctionnelles de cette base de données, la Commission consulte les experts compétents et, lorsqu'elle les met à jour, elle consulte le Comité IA.

2. Les données énumérées à l'annexe VIII, sections A et B, sont introduites dans la base de données de l'UE par le fournisseur ou, le cas échéant, par le mandataire.
3. Les données énumérées à la section C de l'annexe VIII sont introduites dans la base de données de l'UE par le déployeur qui est ou agit pour le compte d'une autorité, d'une agence ou d'un organisme public, conformément à l'article 49, paragraphes 3 et 4.
4. À l'exception de la section visée à l'article 49, paragraphe 4, et à l'article 60, paragraphe 4, point c), les informations contenues dans la base de données de l'UE enregistrées conformément à l'article 49 sont accessibles et mises à la disposition du public d'une manière conviviale. Ces informations devraient être consultables grâce à une navigation aisée et lisibles par machine. Les informations enregistrées conformément à l'article 60 ne sont accessibles qu'aux autorités de surveillance du marché et à la Commission, sauf si le fournisseur ou fournisseur potentiel a donné son consentement pour que ces informations soient également accessibles au public.
5. La base de données de l'UE ne contient des données à caractère personnel que dans la mesure où celles-ci sont nécessaires à la collecte et au traitement d'informations conformément au présent règlement. Ces informations incluent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et légalement autorisées à représenter le fournisseur ou le déployeur, selon le cas.
6. La Commission est la responsable du traitement pour la base de données de l'UE. Elle met à la disposition des fournisseurs, des fournisseurs potentiels et des déployeurs un soutien technique et administratif approprié. La base de données de l'UE est conforme aux exigences applicables en matière d'accessibilité.

Chapitre IX

Surveillance après commercialisation, partage d'informations et surveillance du marché

SECTION 1

SURVEILLANCE APRES COMMERCIALISATION

Article 72

*Surveillance après commercialisation par les fournisseurs
et plan de surveillance après commercialisation pour les systèmes d'IA à haut risque*

1. Les fournisseurs établissent et documentent un système de surveillance après commercialisation d'une manière qui soit proportionnée à la nature des technologies d'IA et des risques du système d'IA à haut risque.
2. Le système de surveillance après commercialisation collecte, documente et analyse, de manière active et systématique, les données pertinentes qui peuvent être fournies par les déployeurs ou qui peuvent être collectées via d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur cycle de vie, et qui permettent au fournisseur d'évaluer si les systèmes d'IA respectent en permanence les exigences énoncées au chapitre III, section 2. Le cas échéant, la surveillance après commercialisation comprend une analyse de l'interaction avec d'autres systèmes d'IA. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs qui sont des autorités répressives.

3. Le système de surveillance après commercialisation repose sur un plan de surveillance après commercialisation. Le plan de surveillance après commercialisation fait partie de la documentation technique visée à l'annexe IV. La Commission adopte un acte d'exécution fixant des dispositions détaillées établissant un modèle pour le plan de surveillance après commercialisation et la liste des éléments à inclure dans le plan au plus tard le ... [18 mois à compter de l'entrée en vigueur du présent règlement]. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.
4. Pour les systèmes d'IA à haut risque relevant de la législation d'harmonisation de l'Union énumérés à la section A de l'annexe I, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de ces actes, afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les éléments nécessaires décrits aux paragraphes 1, 2 et 3 en utilisant le modèle visé au paragraphe 3 dans les systèmes et plans existants au titre desdits actes, pour autant que cela donne lieu à un niveau de protection équivalent.

Le premier alinéa du présent paragraphe s'applique également aux systèmes d'IA à haut risque visés à l'annexe III, point 5, mis sur le marché ou mis en service par des établissements financiers qui sont soumis à des exigences en vertu de la législation de l'Union sur les services financiers concernant leur gouvernance, leurs dispositifs ou leurs processus internes.

SECTION 2

PARTAGE D'INFORMATIONS SUR LES INCIDENTS GRAVES

Article 73

Signalement d'incidents graves

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union signalent tout incident grave aux autorités de surveillance du marché des États membres dans lesquels cet incident s'est produit.
2. Le signalement visé au paragraphe 1 est effectué immédiatement après que le fournisseur a établi un lien de causalité, ou la probabilité raisonnable qu'un tel lien existe, entre le système d'IA et l'incident grave et, en tout état de cause, au plus tard 15 jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

Le délai pour le signalement visé au premier alinéa tient compte de l'ampleur de l'incident grave.

3. Nonobstant le paragraphe 2 du présent article, en cas d'infraction de grande ampleur ou d'incident grave au sens de l'article 3, point 49) b), le signalement visé au paragraphe 1 du présent article est effectué immédiatement, et au plus tard deux jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de cet incident.

4. Nonobstant le paragraphe 2, en cas de décès d'une personne, le signalement est effectué immédiatement après que le fournisseur ou le déployeur a établi un lien de causalité entre le système d'IA à haut risque et l'incident grave ou dès qu'il soupçonne un tel lien, mais au plus tard 10 jours après la date à laquelle le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.
5. Si cela est nécessaire pour assurer un signalement en temps utile, le fournisseur ou, le cas échéant, le déployeur peut soumettre un signalement initial incomplet, suivi d'un signalement complet.
6. À la suite du signalement d'un incident grave en application du paragraphe 1, le fournisseur mène sans tarder les investigations nécessaires liées à l'incident grave et au système d'IA concerné. Ces investigations comprennent notamment une évaluation des risques résultant de l'incident, ainsi que des mesures correctives.

Le fournisseur coopère avec les autorités compétentes et, le cas échéant, avec l'organisme notifié concerné, au cours des investigations visées au premier alinéa, et ne mène aucune investigation nécessitant de modifier le système d'IA concerné d'une manière susceptible d'avoir une incidence sur toute évaluation ultérieure des causes de l'incident, avant d'informer les autorités compétentes de telles mesures.

7. Dès réception d'une notification relative à un incident grave visé à l'article 3, point 49) c), l'autorité de surveillance du marché compétente informe les autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1. La Commission élabore des orientations spécifiques pour faciliter le respect des obligations énoncées au paragraphe 1 du présent article. Ces orientations sont publiées au plus tard le ... [12 mois à compter de l'entrée en vigueur du présent règlement], et font l'objet d'une évaluation régulière.

8. L'autorité de surveillance du marché prend les mesures qui s'imposent, conformément à l'article 19 du règlement (UE) 2019/1020, dans un délai de sept jours à compter de la date à laquelle elle a reçu la notification visée au paragraphe 1 du présent article, et suit les procédures de notification prévues par ledit règlement.
9. Pour les systèmes d'IA à haut risque visés à l'annexe III qui sont mis sur le marché ou mis en service par des fournisseurs qui sont soumis à des instruments législatifs de l'Union établissant des obligations de signalement équivalentes à celles énoncées dans le présent règlement, la notification des incidents graves est limitée à ceux visés à l'article 3, point 49) c).
10. Pour les systèmes d'IA à haut risque qui sont des composants de sécurité de dispositifs, ou qui sont eux-mêmes des dispositifs, relevant des règlements (UE) 2017/745 et (UE) 2017/746, la notification des incidents graves est limitée à ceux qui sont visés à l'article 3, point 49) c), du présent règlement, et est adressée à l'autorité nationale compétente choisie à cette fin par les États membres dans lesquels l'incident s'est produit.
11. Les autorités nationales compétentes notifient immédiatement à la Commission tout incident grave, qu'elles aient ou non pris des mesures à cet égard, conformément à l'article 20 du règlement (UE) 2019/1020.

SECTION 3

CONTROLE DE L'APPLICATION

Article 74

Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union

1. Le règlement (UE) 2019/1020 s'applique aux systèmes d'IA relevant du présent règlement.
Aux fins du contrôle effectif de l'application du présent règlement:
 - a) toute référence à un opérateur économique en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les opérateurs identifiés à l'article 2, paragraphe 1, du présent règlement;
 - b) toute référence à un produit en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les systèmes d'IA relevant du champ d'application du présent règlement.
2. Dans le cadre des obligations d'information qui leur incombent en vertu de l'article 34, paragraphe 4, du règlement (UE) 2019/1020, les autorités de surveillance du marché communiquent chaque année à la Commission et aux autorités nationales de la concurrence concernées toute information recueillie dans le cadre des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de l'Union relatif aux règles de concurrence. Elles font également rapport chaque année à la Commission sur les recours aux pratiques interdites intervenus au cours de l'année concernée et sur les mesures prises.
3. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité responsable des activités de surveillance du marché désignée en vertu de ces actes juridiques.

Par dérogation au premier alinéa, et dans des circonstances appropriées, les États membres peuvent désigner une autre autorité compétente pour faire office d'autorité de surveillance du marché, à condition d'assurer la coordination avec les autorités sectorielles de surveillance du marché compétentes chargées du contrôle de l'application des actes juridiques énumérés à l'annexe I.

4. Les procédures visées aux articles 79 à 83 du présent règlement ne s'appliquent pas aux systèmes d'IA liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure la section A de l'annexe I, lorsque ces actes juridiques prévoient déjà des procédures assurant un niveau de protection équivalent et ayant le même objectif. En pareils cas, ce sont les procédures sectorielles pertinentes qui s'appliquent.
5. Sans préjudice des pouvoirs conférés aux autorités de surveillance du marché par l'article 14 du règlement (UE) 2019/1020, afin d'assurer le contrôle effectif de l'application du présent règlement, les autorités de surveillance du marché peuvent exercer les pouvoirs visés à l'article 14, paragraphe 4, points d) et j), dudit règlement à distance, le cas échéant.
6. Pour les systèmes d'IA à haut risque mis sur le marché, mis en service ou utilisés par des établissements financiers régis par la législation de l'Union sur les services financiers, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité nationale responsable de la surveillance financière de ces établissements en vertu de cette législation dans la mesure où la mise sur le marché, la mise en service ou l'utilisation du système d'IA est directement liée à la fourniture de ces services financiers.

7. Par dérogation au paragraphe 6, dans des circonstances appropriées, et pour autant que la coordination soit assurée, l'État membre peut désigner une autre autorité compétente comme autorité de surveillance du marché aux fins du présent règlement.

Les autorités nationales de surveillance du marché surveillant les établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) n° 1024/2013, devraient communiquer sans tarder à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour les missions de surveillance prudentielle de la Banque centrale européenne définies dans ledit règlement.

8. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, du présent règlement, dans la mesure où ils sont utilisés à des fins répressives, de gestion des frontières et de justice et démocratie, et pour les systèmes d'IA à haut risque énumérés à l'annexe III, points 6, 7 et 8, du présent règlement, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités compétentes en matière de contrôle de la protection des données en vertu du règlement (UE) 2016/679 ou de la directive (UE) 2016/680, soit toute autre autorité désignée en application des mêmes conditions énoncées aux articles 41 à 44 de la directive (UE) 2016/680. Les activités de surveillance du marché ne portent en aucune manière atteinte à l'indépendance des autorités judiciaires ni n'interfèrent d'une autre manière avec leurs activités lorsque ces autorités agissent dans l'exercice de leurs fonctions judiciaires.

9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données est leur autorité de surveillance du marché, sauf en ce qui concerne la Cour de justice de l'Union européenne agissant dans l'exercice de ses fonctions judiciaires.
10. Les États membres facilitent la coordination entre les autorités de surveillance du marché désignées en vertu du présent règlement et les autres autorités ou organismes nationaux compétents pour surveiller l'application de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou dans d'autres législations de l'Union, qui sont susceptibles d'être pertinents pour les systèmes d'IA à haut risque visés à l'annexe III.
11. Les autorités de surveillance du marché et la Commission sont en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener soit par les autorités de surveillance du marché, soit par les autorités de surveillance du marché conjointement avec la Commission, qui ont pour objectif de promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser ou de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont identifiés comme présentant un risque grave dans deux États membres ou plus conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA fournit une aide à la coordination des enquêtes conjointes.

12. Sans préjudice des pouvoirs prévus par le règlement (UE) 2019/1020, et lorsque cela est pertinent et limité à ce qui est nécessaire à l'accomplissement de leurs tâches, les fournisseurs accordent aux autorités de surveillance du marché un accès complet à la documentation ainsi qu'aux jeux de données d'entraînement, de validation et de test utilisés pour le développement des systèmes d'IA à haut risque, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'interfaces de programmation d'application (API) ou d'autres moyens et outils techniques pertinents permettant un accès à distance.
13. Les autorités de surveillance du marché se voient accorder l'accès au code source du système d'IA à haut risque sur demande motivée et uniquement lorsque les deux conditions suivantes sont réunies:
- a) l'accès au code source est nécessaire pour évaluer la conformité d'un système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2; et
 - b) les procédures d'essai ou d'audit et les vérifications fondées sur les données et la documentation communiquées par le fournisseur ont été entièrement accomplies ou se sont révélées insuffisantes.
14. Toute information ou documentation obtenue par les autorités de surveillance du marché est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

Article 75

Assistance mutuelle, surveillance du marché et contrôle des systèmes d'IA à usage général

1. Lorsqu'un système d'IA repose sur un modèle d'IA à usage général, et que le modèle et le système sont mis au point par le même fournisseur, le Bureau de l'IA est habilité à contrôler et surveiller la conformité de ce système d'IA avec les obligations prévues par le présent règlement. Pour s'acquitter de ses tâches de contrôle et de surveillance, le Bureau de l'IA dispose de tous les pouvoirs d'une autorité de surveillance du marché prévus dans la présente section et dans le règlement (UE) 2019/1020.
2. Lorsqu'elles ont des raisons suffisantes de considérer que des systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque en vertu du présent règlement ne sont pas conformes aux exigences énoncées dans le présent règlement, les autorités de surveillance du marché concernées coopèrent avec le Bureau de l'IA pour procéder à des évaluations de la conformité, et en informent le Comité IA et les autres autorités de surveillance du marché.

3. Lorsqu'une autorité de surveillance du marché n'est pas en mesure de conclure son enquête sur le système d'IA à haut risque en raison de son incapacité à accéder à certaines informations relatives au modèle d'IA à usage général bien qu'elle ait déployé tous les efforts appropriés pour obtenir ces informations, elle peut présenter une demande motivée au Bureau de l'IA, par laquelle l'accès à ces informations est mis en œuvre. Dans ce cas, le Bureau de l'IA fournit sans tarder à l'autorité requérante, et en tout état de cause dans un délai de 30 jours, toute information qu'il juge pertinente pour déterminer si un système d'IA à haut risque est non conforme. Les autorités de surveillance du marché garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78 du présent règlement. La procédure prévue au chapitre VI du règlement (UE) 2019/1020 s'applique mutatis mutandis.

Article 76

Supervision des essais en conditions réelles par les autorités de surveillance du marché

1. Les autorités de surveillance du marché ont les compétences et les pouvoirs nécessaires pour veiller à ce que les essais en conditions réelles soient conformes au présent règlement.
2. Lorsque des essais en conditions réelles sont effectués pour des systèmes d'IA supervisés dans un bac à sable réglementaire de l'IA en vertu de l'article 58, les autorités de surveillance du marché vérifient le respect de l'article 60 dans le cadre de leur rôle de surveillance du bac à sable réglementaire de l'IA. Ces autorités peuvent, lorsqu'il y a lieu, autoriser le fournisseur ou le fournisseur potentiel à effectuer les essais en conditions réelles, par dérogation aux conditions énoncées à l'article 60, paragraphe 4, points f) et g).

3. Lorsqu'une autorité de surveillance du marché a été informée d'un incident grave par le fournisseur potentiel, le fournisseur ou tout tiers, ou qu'elle a d'autres raisons de penser que les conditions énoncées aux articles 60 et 61 ne sont pas remplies, elle peut prendre l'une ou l'autre des décisions suivantes sur son territoire, selon le cas:
 - a) suspendre ou faire cesser les essais en conditions réelles;
 - b) exiger du fournisseur ou du fournisseur potentiel et du dépoyeur ou futur dépoyeur qu'ils modifient tout aspect des essais en conditions réelles.
4. Lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3 du présent article, ou a formulé une objection au sens de l'article 60, paragraphe 4, point b), la décision ou l'objection est motivée et indique les modalités selon lesquelles le fournisseur ou le fournisseur potentiel peut contester la décision ou l'objection.
5. Le cas échéant, lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3, elle en communique les motifs aux autorités de surveillance du marché des autres États membres dans lesquels le système d'IA a été testé conformément au plan d'essais.

Article 77

Pouvoirs des autorités de protection des droits fondamentaux

1. Les autorités ou organismes publics nationaux qui supervisent ou font respecter les obligations au titre du droit de l'Union visant à protéger les droits fondamentaux, y compris le droit à la non-discrimination, en ce qui concerne l'utilisation des systèmes d'IA à haut risque visés à l'annexe III sont habilités à demander toute documentation créée ou conservée en vertu du présent règlement et à y avoir accès dans une langue et un format accessibles lorsque l'accès à cette documentation est nécessaire à l'accomplissement effectif de leur mandat dans les limites de leurs compétences. L'autorité ou l'organisme public concerné informe l'autorité de surveillance du marché de l'État membre concerné de toute demande de ce type.
2. Au plus tard le ... [*trois mois à compter de l'entrée en vigueur du présent règlement*], chaque État membre identifie les autorités ou organismes publics visés au paragraphe 1 et met la liste de ces autorités ou organismes à la disposition du public. Les États membres notifient la liste à la Commission et aux autres États membres, et tiennent cette liste à jour.
3. Lorsque la documentation visée au paragraphe 1 ne suffit pas pour déterminer s'il y a eu violation des obligations au titre du droit de l'Union protégeant les droits fondamentaux, l'autorité ou l'organisme public visé au paragraphe 1 peut présenter à l'autorité de surveillance du marché une demande motivée visant à organiser des tests du système d'IA à haut risque par des moyens techniques. L'autorité de surveillance du marché organise les tests avec la participation étroite de l'autorité ou organisme public ayant présenté la demande dans un délai raisonnable après celle-ci.

4. Toute information ou documentation obtenue par les autorités ou organismes publics nationaux visés au paragraphe 1 du présent article en application des dispositions du présent article est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

Article 78
Confidentialité

1. La Commission, les autorités de surveillance du marché et les organismes notifiés, ainsi que toute autre personne physique ou morale associée à l'application du présent règlement respectent, conformément au droit de l'Union ou au droit national, la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier:
- a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil⁵⁷;
 - b) la mise en œuvre effective du présent règlement, notamment en ce qui concerne les inspections, les investigations ou les audits;
 - c) les intérêts en matière de sécurité nationale et publique;
 - d) la conduite des procédures pénales ou administratives;

⁵⁷ Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

- e) les informations classifiées en vertu du droit de l'Union ou du droit national.
2. Les autorités associées à l'application du présent règlement conformément au paragraphe 1 demandent uniquement les données qui sont strictement nécessaires à l'évaluation du risque posé par les systèmes d'IA et à l'exercice de leurs pouvoirs conformément au présent règlement et au règlement (UE) 2019/1020. Elles mettent en place des mesures de cybersécurité adéquates et efficaces pour protéger la sécurité et la confidentialité des informations et des données obtenues, et suppriment les données collectées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été obtenues, conformément au droit de l'Union ou au droit national applicable.
3. Sans préjudice des paragraphes 1 et 2, les informations échangées à titre confidentiel entre les autorités nationales compétentes ou entre celles-ci et la Commission ne sont pas divulguées sans consultation préalable de l'autorité nationale compétente dont elles émanent et du déployeur lorsque les systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, sont utilisés par les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile et lorsque cette divulgation risquerait de porter atteinte aux intérêts en matière de sécurité nationale et publique. Cet échange d'informations ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

Lorsque les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile sont fournisseurs de systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, la documentation technique visée à l'annexe IV reste dans les locaux de ces autorités. Ces autorités veillent à ce que les autorités de surveillance du marché visées à l'article 74, paragraphes 8 et 9, selon le cas, puissent, sur demande, avoir immédiatement accès à la documentation ou en obtenir une copie. Seuls les membres du personnel de l'autorité de surveillance du marché disposant d'une habilitation de sécurité au niveau approprié sont autorisés à avoir accès à cette documentation ou à une copie de celle-ci.

4. Les paragraphes 1, 2 et 3 sont sans effet sur les droits ou obligations de la Commission, des États membres et de leurs autorités compétentes, ainsi que sur les droits ou obligations des organismes notifiés, en matière d'échange d'informations et de diffusion de mises en garde, y compris dans le contexte de la coopération transfrontière, et sur les obligations d'information incombant aux parties concernées en vertu du droit pénal des États membres.
5. La Commission et les États membres peuvent, lorsque cela est nécessaire et conformément aux dispositions pertinentes des accords internationaux et commerciaux, échanger des informations confidentielles avec les autorités de réglementation de pays tiers avec lesquels ils ont conclu des accords bilatéraux ou multilatéraux en matière de confidentialité garantissant un niveau de confidentialité approprié.

Article 79

Procédure applicable au niveau national aux systèmes d'IA présentant un risque

1. On entend par systèmes d'IA présentant un risque, un "produit présentant un risque" au sens de l'article 3, point 19), du règlement (UE) 2019/1020, dans la mesure où ils présentent des risques pour la santé ou la sécurité, ou pour les droits fondamentaux, des personnes.

2. Lorsque l'autorité de surveillance du marché d'un État membre a des raisons suffisantes de considérer qu'un système d'IA présente un risque au sens du paragraphe 1 du présent article, elle procède à une évaluation de la conformité du système d'IA concerné avec l'ensemble des exigences et obligations énoncées dans le présent règlement. Une attention particulière est accordée aux systèmes d'IA présentant un risque pour les groupes vulnérables. Lorsque sont identifiés des risques pour les droits fondamentaux, l'autorité de surveillance du marché informe également les autorités ou organismes publics nationaux concernés visés à l'article 77, paragraphe 1, et coopère pleinement avec eux. Les opérateurs concernés coopèrent, en tant que de besoin, avec l'autorité de surveillance du marché et avec les autres autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1.

Si, au cours de cette évaluation, l'autorité de surveillance du marché ou, le cas échéant, l'autorité de surveillance du marché en coopération avec l'autorité publique nationale visée à l'article 77, paragraphe 1, constate que le système d'IA ne respecte pas les exigences et obligations énoncées dans le présent règlement, elle invite sans retard injustifié l'opérateur concerné à prendre toutes les mesures correctives appropriées pour mettre le système d'IA en conformité, le retirer du marché ou le rappeler dans un délai qu'elle peut prescrire, et en tout état de cause au plus tard dans les 15 jours ouvrables, ou dans un délai prévu par la législation d'harmonisation de l'Union concernée, le délai le plus court étant retenu.

L'autorité de surveillance du marché informe l'organisme notifié concerné en conséquence. L'article 18 du règlement (UE) 2019/1020 s'applique aux mesures visées au deuxième alinéa du présent paragraphe.

3. Lorsque l'autorité de surveillance du marché considère que la non-conformité n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées de l'opérateur.
4. L'opérateur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.
5. Lorsque l'opérateur d'un système d'IA ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2, l'autorité de surveillance du marché prend toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du système d'IA sur son marché national ou sa mise en service, pour retirer le produit ou le système d'IA autonome de ce marché ou pour le rappeler. L'autorité notifie ces mesures sans retard injustifié à la Commission et aux autres États membres.
6. La notification visée au paragraphe 5 contient toutes les précisions disponibles, notamment les informations nécessaires pour identifier le système d'IA non conforme, son origine et la chaîne d'approvisionnement, la nature de la non-conformité alléguée et du risque encouru, ainsi que la nature et la durée des mesures nationales prises et les arguments avancés par l'opérateur concerné. En particulier, l'autorité de surveillance du marché indique si la non-conformité découle d'une ou plusieurs des causes suivantes:
 - a) le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5;
 - b) le non-respect, par le système d'IA à haut risque, des exigences énoncées au chapitre III, section 2;

- c) des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 qui confèrent une présomption de conformité;
 - d) le non-respect de l'article 50.
7. Les autorités de surveillance du marché autres que l'autorité de surveillance du marché de l'État membre qui a entamé la procédure informent sans retard injustifié la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent à propos de la non-conformité du système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.
8. Lorsque, dans les trois mois suivant la réception de la notification visée au paragraphe 5, aucune objection n'a été émise par une autorité de surveillance du marché d'un État membre ou par la Commission à l'encontre d'une mesure provisoire prise par une autorité de surveillance du marché d'un autre État membre, cette mesure est réputée justifiée. Cette disposition est sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020. Le délai de trois mois visé au présent paragraphe est ramené à 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 du présent règlement.
9. Les autorités de surveillance du marché veillent à ce que les mesures restrictives appropriées soient prises sans retard injustifié à l'égard du produit ou du système d'IA concerné, par exemple son retrait de leur marché.

Article 80

Procédure applicable aux systèmes d'IA classés par le fournisseur comme n'étant pas à haut risque en application de l'annexe III

1. Lorsqu'une autorité de surveillance du marché a des raisons suffisantes de considérer qu'un système d'IA classé par le fournisseur comme n'étant pas à haut risque en application de l'article 6, paragraphe 3, est en réalité à haut risque, elle procède à une évaluation du système d'IA concerné quant à la question de sa classification en tant que système d'IA à haut risque sur la base des conditions énoncées à l'article 6, paragraphe 3, et dans les lignes directrices de la Commission.
2. Lorsque, au cours de cette évaluation, l'autorité de surveillance du marché constate que le système d'IA concerné est à haut risque, elle demande sans retard injustifié au fournisseur concerné de prendre toutes les mesures nécessaires pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement, ainsi que de prendre les mesures correctives appropriées dans un délai que l'autorité de surveillance du marché peut prescrire.
3. Lorsque l'autorité de surveillance du marché considère que l'utilisation du système d'IA concerné n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées du fournisseur.

4. Le fournisseur veille à ce que toutes les mesures nécessaires soient prises pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement. Lorsque le fournisseur d'un système d'IA concerné ne met pas le système d'IA en conformité avec ces exigences et obligations dans le délai visé au paragraphe 2 du présent article, il fait l'objet d'amendes conformément à l'article 99.
5. Le fournisseur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.
6. Lorsque le fournisseur du système d'IA concerné ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2 du présent article, l'article 79, paragraphe 5 à 9, s'applique.
7. Lorsque, au cours de l'évaluation prévue au paragraphe 1 du présent article, l'autorité de surveillance du marché établit que le système d'IA a été classé à tort par le fournisseur comme n'étant pas à haut risque afin de contourner l'application des exigences figurant au chapitre III, section 2, le fournisseur fait l'objet d'amendes conformément à l'article 99.
8. Dans l'exercice de leur pouvoir de contrôle de l'application du présent article, et conformément à l'article 11 du règlement (UE) 2019/1020, les autorités de surveillance du marché peuvent effectuer des contrôles appropriés, en tenant compte notamment des informations stockées dans la base de données de l'UE visée à l'article 71 du présent règlement.

Article 81

Procédure de sauvegarde de l'Union

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 79, paragraphe 5, ou dans un délai de 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, l'autorité de surveillance du marché d'un État membre soulève des objections à l'encontre d'une mesure prise par une autre autorité de surveillance du marché, ou que la Commission estime que cette mesure est contraire au droit de l'Union, la Commission entame sans retard injustifié des consultations avec l'autorité de surveillance du marché de l'État membre concerné et le ou les opérateurs, et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission, dans un délai de six mois, ou de 60 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, à compter de la notification visée à l'article 79, paragraphe 5, décide si la mesure nationale est justifiée ou non et communique sa décision à l'autorité de surveillance du marché de l'État membre concerné. La Commission informe également toutes les autres autorités de surveillance du marché de sa décision.
2. Lorsque la Commission estime que la mesure prise par l'État membre concerné est justifiée, tous les États membres veillent à prendre des mesures restrictives appropriées à l'égard du système d'IA concerné, par exemple en exigeant le retrait du système d'IA de leur marché sans retard injustifié, et en informent la Commission. Lorsque la Commission estime que la mesure nationale n'est pas justifiée, l'État membre concerné retire la mesure et en informe la Commission.

3. Lorsque la mesure nationale est jugée justifiée et que la non-conformité du système d'IA est attribuée à des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 du présent règlement, la Commission applique la procédure prévue à l'article 11 du règlement (UE) n° 1025/2012.

Article 82

Systèmes d'IA conformes qui présentent un risque

1. Lorsque, ayant réalisé une évaluation au titre de l'article 79, après avoir consulté l'autorité publique nationale concernée visée à l'article 77, paragraphe 1, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un système d'IA à haut risque soit conforme au présent règlement, il comporte néanmoins un risque pour la santé ou la sécurité des personnes, pour les droits fondamentaux, ou pour d'autres aspects relatifs à la protection de l'intérêt public, elle demande à l'opérateur concerné de prendre toutes les mesures appropriées pour faire en sorte que le système d'IA concerné, une fois mis sur le marché ou mis en service, ne présente plus ce risque, et ce sans retard injustifié, dans un délai qu'elle peut prescrire.
2. Le fournisseur ou autre opérateur concerné s'assure que des mesures correctives sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union dans le délai prescrit par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

3. Les États membres informent immédiatement la Commission et les autres États membres d'une constatation au titre du paragraphe 1. Les informations fournies incluent toutes les précisions disponibles, notamment les données nécessaires à l'identification du système d'IA concerné, l'origine et la chaîne d'approvisionnement de ce système d'IA, la nature du risque encouru, ainsi que la nature et la durée des mesures nationales prises.
4. La Commission entame sans retard injustifié des consultations avec les États membres concernés et les opérateurs concernés, et évalue les mesures nationales prises. En fonction des résultats de cette évaluation, la Commission décide si la mesure est justifiée ou non et, si nécessaire, propose d'autres mesures appropriées.
5. La Commission communique immédiatement sa décision aux États membres concernés ainsi qu'aux opérateurs concernés. Elle en informe également les autres États membres.

Article 83

Non-conformité formelle

1. Lorsque l'autorité de surveillance du marché d'un État membre fait l'une des constatations ci-après, elle invite le fournisseur concerné à mettre un terme à la non-conformité en question, dans un délai qu'elle peut prescrire:
 - a) le marquage CE a été apposé en violation de l'article 48;
 - b) le marquage CE n'a pas été apposé;
 - c) la déclaration UE de conformité visée à l'article 47 n'a pas été établie;

- d) la déclaration UE de conformité visée à l'article 47 n'a pas été établie correctement;
 - e) l'enregistrement dans la base de données de l'UE visée à l'article 71 n'a pas été effectué;
 - f) le cas échéant, il n'a pas été désigné de mandataire;
 - g) la documentation technique n'est pas disponible.
2. Si le cas de non-conformité visé au paragraphe 1 persiste, l'autorité de surveillance du marché de l'État membre concerné prend toutes les mesures appropriées et proportionnées pour restreindre ou interdire la mise à disposition du système d'IA à haut risque sur le marché ou pour assurer son rappel ou son retrait sans tarder du marché.

Article 84

Structures de soutien de l'Union pour les essais en matière d'IA

1. La Commission désigne une ou plusieurs structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 21, paragraphe 6, du règlement (UE) 1020/2019 dans le domaine de l'intelligence artificielle.
2. Sans préjudice des tâches visées au paragraphe 1, les structures de soutien de l'Union pour les essais en matière d'IA fournissent également des avis techniques ou scientifiques indépendants à la demande du Comité IA, de la Commission ou des autorités de surveillance du marché.

SECTION 4

VOIES DE RECOURS

Article 85

Droit d'introduire une réclamation auprès d'une autorité de surveillance du marché

Sans préjudice d'autres recours administratifs ou judiciaires, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement peut déposer des réclamations auprès de l'autorité de surveillance du marché concernée.

Conformément au règlement (UE) 2019/1020, ces réclamations sont prises en compte aux fins de l'exercice des activités de surveillance du marché, et sont traitées conformément aux procédures spécifiques établies en conséquence par les autorités de surveillance du marché.

Article 86

Droit à l'explication des décisions individuelles

1. Toute personne concernée faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un système d'IA à haut risque mentionné à l'annexe III, à l'exception des systèmes énumérés au point 2 de ladite annexe, et qui produit des effets juridiques ou affecte significativement cette personne de façon similaire d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux a le droit d'obtenir du déployeur des explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise.

2. Le paragraphe 1 ne s'applique pas à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions à l'obligation prévue audit paragraphe découlent du droit de l'Union ou du droit national dans le respect du droit de l'Union.
3. Le présent article ne s'applique que dans la mesure où le droit visé au paragraphe 1 n'est pas prévu par ailleurs dans le droit de l'Union.

Article 87

Signalement de violations et protection des auteurs de signalement

La directive (UE) 2019/1937 s'applique aux signalements de violations du présent règlement et à la protection des personnes signalant ces violations.

SECTION 5

SURVEILLANCE, ENQUETES, CONTROLE DE L'APPLICATION ET CONTROLE EN CE QUI CONCERNE LES FOURNISSEURS DE MODELES D'IA A USAGE GENERAL

Article 88

Contrôle de l'exécution des obligations

incombant aux fournisseurs de modèles d'IA à usage général

1. La Commission dispose de pouvoirs exclusifs pour surveiller et contrôler le respect du chapitre V, en tenant compte des garanties procédurales prévues à l'article 94. La Commission confie l'exécution de ces tâches au Bureau de l'IA, sans préjudice des pouvoirs d'organisation dont elle dispose ainsi que de la répartition des compétences entre les États membres et l'Union fondée sur les traités.

2. Sans préjudice de l'article 75, paragraphe 3, les autorités de surveillance du marché peuvent demander à la Commission d'exercer les pouvoirs prévus dans la présente section, lorsque cela est nécessaire et proportionné pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.

Article 89

Mesures de contrôle

1. Aux fins de l'exécution des tâches qui lui sont conférées dans le cadre de la présente section, le Bureau de l'IA peut prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs du présent règlement par les fournisseurs de modèles d'IA à usage général, y compris leur adhésion à des codes de bonne pratique approuvés.
2. Les fournisseurs en aval ont le droit d'introduire une réclamation pour violation du présent règlement. La réclamation est dûment motivée et indique au moins:
 - a) le point de contact du fournisseur du modèle d'IA à usage général concerné;
 - b) une description des faits pertinents, les dispositions concernées du présent règlement et la raison pour laquelle le fournisseur en aval considère que le fournisseur du modèle d'IA à usage général concerné a enfreint le présent règlement;
 - c) toute autre information que le fournisseur en aval qui a envoyé la demande juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

Article 90

Alertes de risques systémiques données par le groupe scientifique

1. Le groupe scientifique peut adresser une alerte qualifiée au Bureau de l'IA lorsqu'il a des raisons de soupçonner:
 - a) qu'un modèle d'IA à usage général présente un risque concret identifiable au niveau de l'Union; ou
 - b) qu'un modèle d'IA à usage général satisfait aux conditions visées à l'article 51.
2. À la suite d'une telle alerte qualifiée, la Commission, par l'intermédiaire du Bureau de l'IA et après en avoir informé le Comité IA, peut exercer les pouvoirs prévus à la présente section aux fins de l'évaluation de la question. Le Bureau de l'IA informe le Comité IA de toute mesure prise conformément aux articles 91 à 94.
3. L'alerte qualifiée est dûment motivée et indique au moins:
 - a) le point de contact du fournisseur du modèle d'IA à usage général concerné présentant un risque systémique;
 - b) une description des faits pertinents et les motifs de l'alerte donnée par le groupe scientifique;
 - c) toute autre information que le groupe scientifique juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

Article 91

Pouvoir de demander de la documentation et des informations

1. La Commission peut demander au fournisseur du modèle d'IA à usage général concerné de fournir la documentation établie par le fournisseur conformément aux articles 53 et 55, ou toute information supplémentaire nécessaire pour évaluer la conformité du fournisseur avec le présent règlement.
2. Avant d'envoyer la demande d'informations, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.
3. Sur demande dûment motivée du groupe scientifique, la Commission peut adresser une demande d'informations au fournisseur d'un modèle d'IA à usage général, lorsque l'accès à ces informations est nécessaire et proportionné pour l'accomplissement des tâches du groupe scientifique au titre de l'article 68, paragraphe 2.
4. La demande d'informations mentionne la base juridique et l'objet de la demande, précise quelles informations sont requises, fixe un délai dans lequel les informations doivent être fournies, et indique les amendes prévues à l'article 101 en cas de fourniture d'informations inexactes, incomplètes ou trompeuses.

5. Le fournisseur du modèle d'IA à usage général concerné, ou son représentant, fournit les informations demandées. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas de personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts fournissent les informations demandées pour le compte du fournisseur du modèle d'IA à usage général concerné. Les avocats dûment habilités à agir peuvent fournir des informations pour le compte de leurs clients. Les clients demeurent néanmoins pleinement responsables si les informations fournies sont incomplètes, inexactes ou trompeuses.

Article 92

Pouvoir de procéder à des évaluations

1. Le Bureau de l'IA, après consultation du Comité IA, peut procéder à des évaluations du modèle d'IA à usage général concerné:
 - a) pour évaluer le respect, par le fournisseur, des obligations prévues par le présent règlement, lorsque les informations recueillies en vertu de l'article 91 sont insuffisantes; ou
 - b) pour enquêter sur les risques systémiques, au niveau de l'Union, des modèles d'IA à usage général présentant un risque systémique, en particulier à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a).
2. La Commission peut décider de désigner des experts indépendants chargés de procéder à des évaluations pour son compte, y compris des experts du groupe scientifique établi en vertu de l'article 68. Les experts indépendants désignés pour cette tâche satisfont aux critères énoncés à l'article 68, paragraphe 2.

3. Aux fins du paragraphe 1, la Commission peut demander l'accès au modèle d'IA à usage général concerné par l'intermédiaire d'API ou d'autres moyens et outils techniques appropriés, y compris le code source.
4. La demande d'accès indique la base juridique, l'objet et les motifs de la demande et fixe le délai dans lequel l'accès doit être accordé, ainsi que les amendes prévues à l'article 101 en cas de non-fourniture de l'accès.
5. Les fournisseurs du modèle d'IA à usage général concerné ou son représentant fournissent les informations requise. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas la personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts, accordent l'accès demandé pour le compte du fournisseur du modèle d'IA à usage général concerné.
6. La Commission adopte des actes d'exécution établissant les modalités détaillées et les conditions des évaluations, y compris les modalités détaillées d'intervention d'experts indépendants, et la procédure relative à leur sélection. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.
7. Avant de demander l'accès au modèle d'IA à usage général concerné, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général afin de recueillir davantage d'informations sur les essais internes du modèle, les garanties internes visant à prévenir les risques systémiques, ainsi que d'autres procédures internes et les mesures que le fournisseur a prises pour atténuer ces risques.

Article 93

Pouvoir de demander des mesures

1. Lorsque cela est nécessaire et approprié, la Commission peut demander aux fournisseurs:
 - a) de prendre les mesures appropriées pour se conformer aux obligations énoncées à aux articles 53 et 54;
 - b) de mettre en œuvre des mesures d'atténuation, lorsque l'évaluation effectuée conformément à l'article 92 a suscité des préoccupations sérieuses et fondées quant à un risque systémique au niveau de l'Union;
 - c) de restreindre la mise à disposition du modèle sur le marché, de le retirer ou de le rappeler.
2. Avant qu'une mesure ne soit demandée, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.
3. Si, au cours du dialogue structuré visé au paragraphe 2, le fournisseur du modèle d'IA à usage général présentant un risque systémique s'engage à mettre en œuvre des mesures d'atténuation pour faire face à un risque systémique au niveau de l'Union, la Commission peut, par une décision, rendre ces engagements contraignants et déclarer qu'il n'y a plus lieu d'agir.

Article 94

Droits procéduraux des opérateurs économiques du modèle d'IA à usage général

L'article 18 du règlement (UE) 2019/1020 s'applique mutatis mutandis aux fournisseurs du modèle d'IA à usage général, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

Chapitre X

Codes de conduite et lignes directrices

Article 95

Codes de conduite pour l'application volontaire de certaines exigences

1. Le Bureau de l'IA et les États membres encouragent et facilitent l'élaboration de codes de conduite, comportant des mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire, aux systèmes d'IA autres que les systèmes d'IA à haut risque, de tout ou partie des exigences énoncées au chapitre III, section 2, en tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur permettant l'application de ces exigences.

2. Le Bureau de l'IA et les États membres facilitent l'élaboration de codes de conduite concernant l'application volontaire, y compris par les déployeurs, d'exigences spécifiques à tous les systèmes d'IA, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que, entre autres:
- a) les éléments applicables prévus dans les lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance;
 - b) l'évaluation et la réduction au minimum de l'incidence des systèmes d'IA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficaces de l'IA;
 - c) la promotion de la maîtrise de l'IA, en particulier chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA;
 - d) la facilitation d'une conception inclusive et diversifiée des systèmes d'IA, notamment par la mise en place d'équipes de développement inclusives et diversifiées et la promotion de la participation des parties prenantes à ce processus;
 - e) l'évaluation et la prévention de l'impact négatif des systèmes d'IA sur les personnes ou groupes de personnes vulnérables, y compris en ce qui concerne l'accessibilité pour les personnes handicapées, ainsi que sur l'égalité de genre.

3. Les codes de conduite peuvent être élaborés par des fournisseurs ou déployeurs individuels de systèmes d'IA ou par des organisations les représentant ou par les deux, y compris avec la participation de toute partie intéressée et de leurs organisations représentatives, y compris des organisations de la société civile et le monde universitaire. Les codes de conduite peuvent porter sur un ou plusieurs systèmes d'IA, compte tenu de la similarité de la destination des systèmes concernés.
4. Le Bureau de l'IA et les États membres prennent en considération les intérêts et les besoins spécifiques des PME, y compris les jeunes pousses, lorsqu'ils encouragent et facilitent l'élaboration de codes de conduite.

Article 96

Lignes directrices de la Commission sur la mise en œuvre du présent règlement

1. La Commission élabore des lignes directrices sur la mise en œuvre pratique du présent règlement, et en particulier sur:
 - a) l'application des exigences et obligations visées aux articles 8 à 15 et à l'article 25;
 - b) les pratiques interdites visées à l'article 5;
 - c) la mise en œuvre pratique des dispositions relatives aux modifications substantielles;
 - d) la mise en œuvre pratique des obligations de transparence prévues à l'article 50;

- e) des informations détaillées sur la relation entre le présent règlement et la législation d'harmonisation de l'Union dont la liste figure à l'annexe I ainsi que d'autres actes législatifs pertinents de l'Union, y compris en ce qui concerne la cohérence de leur application;
- f) l'application de la définition d'un système d'IA telle qu'elle figure à l'article 3, point 1).

Lorsqu'elle publie ces lignes directrices, la Commission accorde une attention particulière aux besoins des PME, y compris les jeunes pousses, des pouvoirs publics locaux et des secteurs les plus susceptibles d'être affectés par le présent règlement.

Les lignes directrices visées au premier alinéa du présent paragraphe tiennent dûment compte de l'état de la technique généralement reconnu en matière d'IA, ainsi que des normes harmonisées et spécifications communes pertinentes visées aux articles 40 et 41, ou des normes harmonisées ou spécifications techniques qui sont énoncées en vertu de la législation d'harmonisation de l'Union.

- 2. À la demande des États membres ou du Bureau de l'IA, ou de sa propre initiative, la Commission met à jour les lignes directrices précédemment adoptées lorsque cela est jugé nécessaire.

Chapitre XI

Délégation de pouvoir et procédure de comité

Article 97

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.
2. Le pouvoir d'adopter des actes délégués visé à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, est conféré à la Commission pour une durée de cinq ans à partir du ... [date d'entrée en vigueur du présent règlement]. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.
3. La délégation de pouvoir visée à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer".
5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.
6. Un acte délégué adopté en vertu de l'article 6, paragraphe 6 ou 7, de l'article 7, paragraphe 1 ou 3, de l'article 11, paragraphe 3, de l'article 43, paragraphe 5 ou 6, de l'article 47, paragraphe 5, de l'article 51, paragraphe 3, de l'article 52, paragraphe 4, ou de l'article 53, paragraphe 5 ou 6, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 98

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.
2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Chapitre XII

Sanctions

Article 99

Sanctions

1. Conformément aux conditions établies dans le présent règlement, les États membres déterminent le régime des sanctions et autres mesures d'exécution, qui peuvent également comprendre des avertissements et des mesures non monétaires, applicables aux violations du présent règlement commises par des opérateurs, et prennent toute mesure nécessaire pour veiller à la mise en œuvre correcte et effective de ces sanctions, tenant ainsi compte des lignes directrices publiées par la Commission en vertu de l'article 96. Ces sanctions doivent être effectives, proportionnées et dissuasives. Elles tiennent compte des intérêts des PME, y compris les jeunes pousses, et de leur viabilité économique.
2. Les États membres informent la Commission, sans retard et au plus tard à la date d'entrée en application, du régime des sanctions et des autres mesures d'exécution visées au paragraphe 1, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.
3. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'amendes administratives pouvant aller jusqu'à 35 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 7 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

4. La non-conformité avec l'une quelconque des dispositions suivantes relatives aux opérateurs ou aux organismes notifiés, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 3 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu:
- a) les obligations incombant aux fournisseurs en vertu de l'article 16;
 - b) les obligations incombant aux mandataires en vertu de l'article 22;
 - c) les obligations incombant aux importateurs en vertu de l'article 23;
 - d) les obligations incombant aux distributeurs en vertu de l'article 24;
 - e) les obligations incombant aux dépoyeurs en vertu de l'article 26;
 - f) les exigences et obligations applicables aux organismes notifiés en application de l'article 31, de l'article 33, paragraphes 1, 3 et 4, ou de l'article 34;
 - g) les obligations de transparence pour les fournisseurs et les dépoyeurs conformément à l'article 50.
5. La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales compétentes en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 7 500 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 1 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.
6. Dans le cas des PME, y compris les jeunes pousses, chaque amende visée au présent article s'élève au maximum aux pourcentages ou montants visés aux paragraphes 3, 4 et 5, le chiffre le plus faible étant retenu.

7. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et, le cas échéant, il est tenu compte des éléments suivants:
- a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné, ainsi que, le cas échéant, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;
 - b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour la même violation;
 - c) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités au même opérateur pour des violations d'autres dispositions du droit de l'Union ou du droit national, lorsque ces violations résultent de la même activité ou omission constituant une violation pertinente au sens du présent règlement;
 - d) la taille, le chiffre d'affaires annuel et la part de marché de l'opérateur qui commet la violation;
 - e) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation;
 - f) le degré de coopération établi avec les autorités nationales compétentes en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

- g) le degré de responsabilité de l'opérateur, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;
 - h) la manière dont les autorités nationales compétentes ont eu connaissance de la violation, notamment si, et dans quelle mesure, l'opérateur a notifié la violation;
 - i) le fait que la violation a été commise délibérément ou par négligence;
 - j) toute mesure prise par l'opérateur pour atténuer le préjudice subi par les personnes concernées.
8. Chaque État membre établit les règles déterminant dans quelle mesure des amendes administratives peuvent être imposées à des autorités et organismes publics établis sur son territoire.
9. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que les amendes sont imposées par les juridictions nationales compétentes ou par d'autres organismes, selon le cas prévu dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.
10. L'exercice des pouvoirs conférés par le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit national, y compris des recours juridictionnels effectifs et une procédure régulière.
11. Les États membres font rapport chaque année à la Commission sur les amendes administratives qu'ils ont infligées au cours de l'année concernée, conformément au présent article, ainsi que sur toute action en justice ou procédure judiciaire connexe.

Article 100

Amendes administratives imposées aux institutions, organes et organismes de l'Union

1. Le Contrôleur européen de la protection des données peut imposer des amendes administratives aux institutions, organes et organismes de l'Union relevant du champ d'application du présent règlement. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et il est dûment tenu compte des éléments suivants:
 - a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné ainsi que, s'il y a lieu, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;
 - b) le degré de responsabilité de l'institution, organe ou organisme de l'Union, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;
 - c) toute mesure prise par l'institution, organe ou organisme de l'Union pour atténuer les dommages subis par les personnes touchées;
 - d) le niveau de coopération établi avec le Contrôleur européen de la protection des données en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs, y compris le respect de toute mesure précédemment ordonnée par le Contrôleur européen de la protection des données à l'encontre de l'institution, organe ou organisme de l'Union concerné pour le même objet;

- e) toute violation similaire commise précédemment par l'institution, organe ou organisme de l'Union;
 - f) la manière dont le Contrôleur européen de la protection des données a eu connaissance de la violation, notamment si, et le cas échéant dans quelle mesure, l'institution, organe ou organisme de l'Union a notifié la violation;
 - g) le budget annuel de l'institution, organe ou organisme de l'Union.
- 2. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'une amende administrative pouvant aller jusqu'à 1 500 000 EUR.
 - 3. La non-conformité du système d'IA avec les exigences ou obligations au titre du présent règlement, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 750 000 EUR.
 - 4. Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution, organe ou organisme de l'Union faisant l'objet des procédures conduites par le Contrôleur européen de la protection des données la possibilité de faire connaître son point de vue sur l'éventuelle infraction. Le Contrôleur européen de la protection des données ne fonde ses décisions que sur les éléments et les circonstances au sujet desquels les parties concernées ont pu formuler des observations. Les éventuels plaignants sont étroitement associés à la procédure.

5. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.
6. Les fonds collectés en imposant des amendes en vertu du présent article contribuent au budget général de l'Union. Les amendes ne compromettent pas le bon fonctionnement de l'institution, organe ou organisme de l'Union faisant l'objet d'une amende.
7. Le Contrôleur européen de la protection des données informe chaque année la Commission des amendes administratives qu'il a infligées en vertu du présent article ainsi que de toute action en justice ou procédure judiciaire qu'il a engagée.

Article 101

Amendes applicables aux fournisseurs de modèles d'IA à usage général

1. La Commission peut infliger aux fournisseurs de modèles d'IA à usage général des amendes n'excédant pas 3 % de leur chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, ou 15 000 000 d'euros, le montant le plus élevé étant retenu, lorsque la Commission constate que le fournisseur, de manière délibérée ou par négligence:
 - a) a enfreint les dispositions pertinentes du présent règlement;
 - b) n'a pas donné suite à une demande de document ou d'informations au titre de l'article 91, ou a fourni des informations inexactes, incomplètes ou trompeuses;

- c) ne s'est pas conformé à une mesure demandée au titre de l'article 93;
- d) n'a pas donné à la Commission accès au modèle d'IA à usage général ou au modèle d'IA à usage général présentant un risque systémique en vue de procéder à une évaluation conformément à l'article 92.

Pour fixer le montant de l'amende ou de l'astreinte, il y a lieu de prendre en considération la nature, la gravité et la durée de la violation, tout en tenant dûment compte des principes de proportionnalité et d'adéquation. La Commission tient également compte des engagements pris conformément à l'article 93, paragraphe 3, ou pris dans les codes de bonne pratique pertinents conformément à l'article 56.

- 2. Avant d'adopter la décision en vertu du paragraphe 1, la Commission communique ses constatations préliminaires au fournisseur du modèle d'IA à usage général, et lui donne la possibilité d'être entendu.
- 3. Les amendes infligées conformément au présent article sont effectives, proportionnées et dissuasives.
- 4. Les informations relatives aux amendes infligées en vertu du présent article sont en outre communiquées au Comité IA, le cas échéant.
- 5. La Cour de justice de l'Union européenne statue avec compétence de pleine juridiction sur les recours formés contre les décisions par lesquelles la Commission a fixé une amende au titre du présent article. Elle peut supprimer, réduire ou majorer l'amende infligée.

6. La Commission adopte des actes d'exécution contenant les modalités détaillées des procédures et des garanties procédurales en vue de l'adoption éventuelle de décisions en vertu du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Chapitre XIII

Dispositions finales

Article 102

Modification du règlement (CE) n° 300/2008

À l'article 4, paragraphe 3, du règlement (CE) n° 300/2008, l'alinéa suivant est ajouté:

"Lors de l'adoption de mesures détaillées relatives aux spécifications techniques et aux procédures d'approbation et d'utilisation des équipements de sûreté en ce qui concerne les systèmes d'intelligence artificielle au sens du règlement (UE) 2024/... du Parlement européen et du Conseil⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...)."

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 103

Modification du règlement (UE) n° 167/2013

À l'article 17, paragraphe 5, du règlement (UE) n° 167/2013, l'alinéa suivant est ajouté:

"Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...)."

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 104

Modification du règlement (UE) n° 168/2013

À l'article 22, paragraphe 5, du règlement (UE) n° 168/2013, l'alinéa suivant est ajouté:

"Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...).".

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 105

Modification de la directive 2014/90/UE

À l'article 8 de la directive 2014/90/UE, le paragraphe suivant est ajouté:

- "5. Pour les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil^{*,} lorsqu'elle exerce ses activités conformément au paragraphe 1 et qu'elle adopte des spécifications techniques et des normes d'essai conformément aux paragraphes 2 et 3, la Commission tient compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...).".

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 106

Modification de la directive (UE) 2016/797

À l'article 5 de la directive (UE) 2016/797, le paragraphe suivant est ajouté:

- "12. Lors de l'adoption d'actes délégués conformément au paragraphe 1 et d'actes d'exécution conformément au paragraphe 11 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...)."

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 107
Modification du règlement (UE) 2018/858

À l'article 5 du règlement (UE) 2018/858, le paragraphe suivant est ajouté:

- "4. Lors de l'adoption d'actes délégués conformément au paragraphe 3 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil^{*,+}, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...).".

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 108
Modifications du règlement (UE) 2018/1139

Le règlement (UE) 2018/1139 est modifié comme suit:

1) À l'article 17, le paragraphe suivant est ajouté:

"3. Sans préjudice du paragraphe 2, lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil^{*,} il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...).".

2) À l'article 19, le paragraphe suivant est ajouté:

"4. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/...⁺⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement."

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

⁺⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)).

3) À l'article 43, le paragraphe suivant est ajouté:

"4. Lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/...⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement."

4) À l'article 47, le paragraphe suivant est ajouté:

"3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/...⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement."

5) À l'article 57, le paragraphe suivant est ajouté:

"Lors de l'adoption de ces actes d'exécution en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/...⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement."

6) À l'article 58, le paragraphe suivant est ajouté:

"3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/...⁺, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement."

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)).

Article 109
Modification du règlement (UE) 2019/2144

À l'article 11 du règlement (UE) 2019/2144, le paragraphe suivant est ajouté:

- "3. Lors de l'adoption d'actes d'exécution conformément au paragraphe 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/... du Parlement européen et du Conseil^{*,+}, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

* Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, ..., ELI: ...).".

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Article 110
Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828 du Parlement européen et du Conseil⁵⁸, le point suivant est ajouté:

"68) Règlement (UE) 2024/... du Parlement européen et du Conseil du ... établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)⁺ (JO L, ..., ELI: ...).".

Article 111
Systèmes d'IA déjà mis sur le marché ou mis en service
et modèles d'IA à usage général déjà mis sur le marché

1. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), les systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe X et mis sur le marché ou mis en service avant le ... [36 mois à compter de la date d'entrée en vigueur du présent règlement] sont mis en conformité avec le présent règlement au plus tard le 31 décembre 2030.

⁵⁸ Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement PE-CONS 24/24 (2021/0106 (COD)) et compléter la note de bas de page correspondante.

Il est tenu compte des exigences énoncées dans le présent règlement lors de l'évaluation de chaque système d'information à grande échelle établi par les actes juridiques énumérés à l'annexe X devant être effectuée conformément à ces actes juridiques et lorsque ces actes juridiques sont remplacés ou modifiés.

2. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), le présent règlement s'applique aux opérateurs de systèmes d'IA à haut risque, autres que les systèmes visés au paragraphe 1 du présent article, qui ont été mis sur le marché ou mis en service avant le ... *[24 mois à compter de la date d'entrée en vigueur du présent règlement]*, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leurs conceptions. En tout état de cause, les fournisseurs et les dépoyeurs de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques prennent les mesures nécessaires pour se conformer aux exigences et obligations du présent règlement au plus tard le ... *[six ans à compter de la date d'entrée en vigueur du présent règlement]*.
3. Les fournisseurs de modèles d'IA à usage général qui ont été mis sur le marché avant le ... *[12 mois à compter de la date d'entrée en vigueur du présent règlement]* prennent les mesures nécessaires pour se conformer aux obligations prévues par le présent règlement au plus tard le ... *[36 mois à compter de la date d'entrée en vigueur du présent règlement]*.

Article 112

Évaluation et réexamen

1. La Commission évalue la nécessité de modifier la liste figurant à l'annexe III et la liste des pratiques d'IA interdites figurant à l'article 5, une fois par an après l'entrée en vigueur du présent règlement et jusqu'à la fin de la période de délégation de pouvoir énoncée à l'article 97. La Commission transmet les conclusions de cette évaluation au Parlement européen et au Conseil.
2. Au plus tard le ... [*quatre ans à compter de la date d'entrée en vigueur du présent règlement*] et tous les quatre ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen et au Conseil sur les éléments suivants:
 - a) la nécessité de modifications pour étendre des rubriques de domaine existantes ou ajouter de nouvelles rubriques de domaine dans l'annexe III;
 - b) les modifications de la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires au titre de l'article 50;
 - c) les modifications visant à renforcer l'efficacité du système de surveillance et de gouvernance.

3. Au plus tard le ... [*cinq ans à compter de la date d'entrée en vigueur du présent règlement*] et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Le rapport comprend une évaluation en ce qui concerne la structure de contrôle de l'application ainsi que l'éventuelle nécessité d'une agence de l'Union pour remédier aux lacunes identifiées. Sur la base des constatations, ce rapport est, le cas échéant, accompagné d'une proposition de modification du présent règlement. Les rapports sont publiés.
4. Les rapports visés au paragraphe 2 prêtent une attention particulière aux éléments suivants:
- a) l'état des ressources financières, techniques et humaines dont les autorités nationales compétentes ont besoin pour mener efficacement à bien les missions qui leur sont dévolues par le présent règlement;
 - b) l'état des sanctions, notamment les amendes administratives visées à l'article 99, paragraphe 1, appliquées par les États membres en cas de violation du présent règlement;
 - c) les normes harmonisées adoptées et les spécifications communes élaborées à l'appui du présent règlement;
 - d) le nombre d'entreprises qui arrivent sur le marché après l'entrée en application du présent règlement, et combien d'entre elles sont des PME.

5. Au plus tard le ... [*quatre ans à compter de la date d'entrée en vigueur du présent règlement*], la Commission évalue le fonctionnement du Bureau de l'IA, afin de déterminer si des pouvoirs et compétences suffisants lui ont été conférés pour s'acquitter de ses tâches, et s'il serait pertinent et nécessaire pour la bonne mise en œuvre et l'application correcte du présent règlement de renforcer le Bureau de l'IA et ses compétences d'exécution et d'accroître ses ressources. La Commission présente un rapport sur son évaluation au Parlement européen et au Conseil.
6. Au plus tard le ... [*quatre ans à compter de la date d'entrée en vigueur du présent règlement*] et tous les quatre ans par la suite, la Commission présente un rapport sur l'examen de l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, et évalue la nécessité de mesures ou d'actions supplémentaires, y compris de mesures ou d'actions contraignantes. Ce rapport est présenté au Parlement européen et au Conseil et il est rendu public.
7. Au plus tard le ... [*quatre ans à compter de la date d'entrée en vigueur du présent règlement*] et tous les trois ans par la suite, la Commission évalue l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées au chapitre III, section 2, pour les systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à haut risque, y compris en ce qui concerne la durabilité environnementale.
8. Aux fins des paragraphes 1 à 7, le Comité IA, les États membres et les autorités nationales compétentes fournissent des informations à la Commission à la demande de cette dernière et sans retard injustifié.

9. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 à 7, la Commission tient compte des positions et des conclusions du Comité IA, du Parlement européen, du Conseil et d'autres organismes ou sources pertinents.
10. La Commission soumet, si nécessaire, des propositions appropriées visant à modifier le présent règlement, notamment en tenant compte de l'évolution des technologies, de l'effet des systèmes d'IA sur la santé et la sécurité, ainsi que sur les droits fondamentaux, et à la lumière de l'état d'avancement de la société de l'information.
11. Pour orienter les évaluations et les réexamens visés aux paragraphes 1 à 7 du présent article, le Bureau de l'IA entreprend de mettre au point une méthode objective et participative pour l'évaluation des niveaux de risque fondée sur les critères décrits dans les articles pertinents et l'inclusion de nouveaux systèmes dans:
- a) la liste figurant à l'annexe III, y compris l'extension des rubriques de domaine existantes ou l'ajout de nouvelles rubriques de domaine dans ladite annexe;
 - b) la liste des pratiques interdites figurant à l'article 5; et
 - c) la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires en application de l'article 50.
12. Toute modification du présent règlement en vertu du paragraphe 10, ou tout acte délégué ou acte d'exécution pertinent, qui concerne la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, tient compte des spécificités réglementaires de chaque secteur, ainsi et des mécanismes de gouvernance, d'évaluation de la conformité et d'applications existants et des autorités qui y sont établies.

13. Au plus tard le ... [*sept ans à compter de la date d'entrée en vigueur du présent règlement*], la Commission procède à une évaluation de sa mise en application dont elle fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte des premières années d'application du présent règlement. Sur la base des conclusions, ce rapport est accompagné, le cas échéant, d'une proposition de modification du présent règlement en ce qui concerne la structure de contrôle de l'application ainsi que la nécessité d'une agence de l'Union pour remédier aux lacunes identifiées.

Article 113

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du ... [*24 mois à compter de la date d'entrée en vigueur du présent règlement*].

Toutefois:

- a) Les chapitres I et II sont applicables à partir du ... [*six mois à compter de la date d'entrée en vigueur du présent règlement*];
- b) Le chapitre III, section 4, le chapitre V, le chapitre VII, le chapitre XII et l'article 78 s'appliquent à partir du ... [*12 mois à compter de la date d'entrée en vigueur du présent règlement*], à l'exception de l'article 101;

- c) L'article 6, paragraphe 1, et les obligations correspondantes du présent règlement s'appliquent à partir du ... [36 mois après l'entrée en vigueur du présent règlement].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen

La présidente

Par le Conseil

Le président/La présidente

ANNEXE I

Liste de la législation d'harmonisation de l'Union

Section A. Liste de la législation d'harmonisation de l'Union fondée sur le nouveau cadre législatif

1. Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24);
2. Directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets (JO L 170 du 30.6.2009, p. 1);
3. Directive 2013/53/UE du Parlement européen et du Conseil du 20 novembre 2013 relative aux bateaux de plaisance et aux véhicules nautiques à moteur et abrogeant la directive 94/25/CE (JO L 354 du 28.12.2013, p. 90);
4. Directive 2014/33/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les ascenseurs et les composants de sécurité pour ascenseurs (JO L 96 du 29.3.2014, p. 251);
5. Directive 2014/34/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles (JO L 96 du 29.3.2014, p. 309);

6. Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62);
7. Directive 2014/68/UE du Parlement européen et du Conseil du 15 mai 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des équipements sous pression (JO L 189 du 27.6.2014, p. 164);
8. Règlement (UE) 2016/424 du Parlement européen et du Conseil du 9 mars 2016 relatif aux installations à câbles et abrogeant la directive 2000/9/CE (JO L 81 du 31.3.2016, p. 1);
9. Règlement (UE) 2016/425 du Parlement européen et du Conseil du 9 mars 2016 relatif aux équipements de protection individuelle et abrogeant la directive 89/686/CEE du Conseil (JO L 81 du 31.3.2016, p. 51);
10. Règlement (UE) 2016/426 du Parlement européen et du Conseil du 9 mars 2016 concernant les appareils brûlant des combustibles gazeux et abrogeant la directive 2009/142/CE (JO L 81 du 31.3.2016, p. 99);
11. Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1);

12. Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

Section B. Liste des autres législations d'harmonisation de l'Union

13. Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72);
14. Règlement (UE) n° 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52);
15. Règlement (UE) n° 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1);
16. Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146);
17. Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44);

18. Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1);
19. Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1);

20. Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil et le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1), dans la mesure où il concerne la conception, la production et la mise sur le marché des aéronefs visés à son article 2, paragraphe 1, points a) et b), lorsque cela concerne des aéronefs sans équipage à bord et leurs moteurs, hélices, pièces et équipements de contrôle à distance.
-

ANNEXE II

Liste des infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii)

Infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii):

- terrorisme,
- traite des êtres humains,
- exploitation sexuelle des enfants et pédopornographie,
- trafic de stupéfiants ou de substances psychotropes,
- trafic d'armes, de munitions ou d'explosifs,
- homicide volontaire, coups et blessures graves,
- trafic d'organes ou de tissus humains,
- trafic de matières nucléaires ou radioactives,
- enlèvement, séquestration ou prise d'otage,
- crimes relevant de la compétence de la Cour pénale internationale,
- détournement d'avion ou de navire,

- viol,
 - criminalité environnementale,
 - vol organisé ou à main armée,
 - sabotage,
 - participation à une organisation criminelle impliquée dans une ou plusieurs des infractions énumérées ci-dessus.
-

ANNEXE III

Systèmes d'IA à haut risque visés à l'article 6, paragraphe 2

Les systèmes d'IA à haut risque au sens de l'article 6, paragraphe 2, sont les systèmes d'IA répertoriés dans l'un des domaines suivants:

1. Biométrie, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:
 - a) systèmes d'identification biométrique à distance.

Cela n'inclut pas les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique dont la seule finalité est de confirmer qu'une personne physique spécifique est la personne qu'elle prétend être;
 - b) systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique, en fonction d'attributs ou de caractéristiques sensibles ou protégés, sur la base de la déduction de ces attributs ou de ces caractéristiques;
 - c) systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions.
2. Infrastructures critiques: systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité.

3. Éducation et formation professionnelle:

- a) systèmes d'IA destinés à être utilisés pour déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement et de formation professionnelle, à tous les niveaux;
- b) systèmes d'IA destinés à être utilisés pour évaluer les acquis d'apprentissage, y compris lorsque ceux-ci sont utilisés pour orienter le processus d'apprentissage de personnes physiques dans les établissements d'enseignement et de formation professionnelle, à tous les niveaux;
- c) systèmes d'IA destinés à être utilisés pour évaluer le niveau d'enseignement approprié qu'une personne recevra ou sera en mesure d'atteindre, dans le contexte ou au sein d'établissements d'enseignement et de formation professionnelle à tous les niveaux;
- d) systèmes d'IA destinés à être utilisés pour surveiller et détecter des comportements interdits chez les étudiants lors d'examens dans le contexte d'établissements d'enseignement et de formation ou en leur sein à tous les niveaux;

4. Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant:

- a) systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, en particulier pour publier des offres d'emploi ciblées, analyser et filtrer les candidatures et évaluer les candidats;

- b) systèmes d'IA destinés à être utilisés pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations.

5. Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels:

- a) systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soins de santé, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services;
- b) systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières;
- c) systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie;
- d) systèmes d'IA destinés à évaluer et hiérarchiser les appels d'urgence émanant de personnes physiques ou à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par la police, les pompiers et l'assistance médicale, ainsi que pour les systèmes de tri des patients admis dans les services de santé d'urgence.

6. Répression, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:
- a) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives ou en leur nom pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales;
 - b) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives, en tant que polygraphes ou outils similaires;
 - c) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales;
 - d) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer le risque qu'une personne physique commette une infraction ou récidive, sans se fonder uniquement sur le profilage des personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes;

- e) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre de la détection d'infractions pénales, d'enquêtes ou de poursuites en la matière ou de l'exécution de sanctions pénales.

7. Migration, asile et gestion des contrôles aux frontières, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

- a) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, en tant que polygraphes et outils similaires;
- b) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour évaluer un risque, y compris un risque pour la sécurité, un risque de migration irrégulière ou un risque pour la santé, posé par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre;
- c) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour aider les autorités publiques compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, y compris les évaluations connexes de la fiabilité des éléments de preuve;

- d) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques, à l'exception de la vérification des documents de voyage.

8. Administration de la justice et processus démocratiques:

- a) systèmes d'IA destinés à être utilisés par les autorités judiciaires ou en leur nom, pour les aider à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits, ou à être utilisés de manière similaire lors du règlement extrajudiciaire d'un litige;
- b) systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums. Sont exclus les systèmes d'IA aux sorties desquels les personnes physiques ne sont pas directement exposées, tels que les outils utilisés pour organiser, optimiser ou structurer les campagnes politiques sous l'angle administratif ou logistique.

ANNEXE IV

Documentation technique visée à l'article 11, paragraphe 1

La documentation technique visée à l'article 11, paragraphe 1, contient au moins les informations ci-après, selon le système d'IA concerné:

1. une description générale du système d'IA, y compris:
 - a) la destination, le nom du fournisseur et la version du système, faisant apparaître sa relation aux versions précédentes;
 - b) la manière dont le système d'IA interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels, y compris avec d'autres systèmes d'IA, qui ne font pas partie du système d'IA lui-même, le cas échéant;
 - c) les versions des logiciels ou des micrologiciels pertinents et toute exigence relative aux mises à jour de la version;
 - d) la description de toutes les formes sous lesquelles le système d'IA est mis sur le marché ou mis en service, telles que les packs logiciels intégrés dans du matériel informatique, les téléchargements ou les API;
 - e) la description du matériel informatique sur lequel le système d'IA est destiné à être exécuté;
 - f) lorsque le système d'IA est un composant de produits, des photographies ou des illustrations montrant les caractéristiques externes, le marquage et la disposition interne de ces produits;

- g) une description de base de l'interface utilisateur fournie au déployeur;
 - h) une notice d'utilisation à l'intention du déployeur et une description de base de l'interface utilisateur fournie au déployeur, le cas échéant;
2. une description détaillée des éléments du système d'IA et de son processus de développement, y compris:
- a) les méthodes et étapes suivies pour le développement du système d'IA, y compris, le cas échéant, le recours à des systèmes ou outils pré-entraînés fournis par des tiers et la manière dont ceux-ci ont été utilisés, intégrés ou modifiés par le fournisseur;
 - b) les spécifications de conception du système, à savoir la logique générale du système d'IA et des algorithmes; les principaux choix de conception, y compris le raisonnement et les hypothèses retenues, y compris en ce qui concerne les personnes ou les groupes de personnes à l'égard desquels le système est destiné à être utilisé; les principaux choix de classification; ce que le système est conçu pour optimiser, ainsi que la pertinence des différents paramètres; la description des sorties attendues du système et de leur qualité; les décisions relatives aux compromis éventuels en ce qui concerne les solutions techniques adoptées pour se conformer aux exigences énoncées au chapitre III, section 2;
 - c) la description de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global; les ressources informatiques utilisées pour développer, entraîner, mettre à l'essai et valider le système d'IA;

- d) le cas échéant, les exigences relatives aux données en ce qui concerne les fiches décrivant les méthodes et techniques d'entraînement et les jeux de données d'entraînement utilisés, y compris une description générale de ces jeux de données et des informations sur leur provenance, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées; les procédures d'étiquetage (par exemple pour l'apprentissage supervisé), les méthodes de nettoyage des données (par exemple la détection des valeurs aberrantes);
- e) l'évaluation des mesures de contrôle humain nécessaires conformément à l'article 14, y compris une évaluation des mesures techniques nécessaires pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA, conformément à l'article 13, paragraphe 3, point d);
- f) le cas échéant, une description détaillée des modifications prédéterminées du système d'IA et de ses performances, ainsi que toutes les informations pertinentes relatives aux solutions techniques adoptées pour garantir que continue d'être assurée la conformité du système d'IA aux exigences pertinentes énoncées au chapitre III, section 2;
- g) les procédures de validation et d'essai utilisées, y compris les informations sur les données de validation et d'essai utilisées et leurs principales caractéristiques; les indicateurs utilisés pour mesurer l'exactitude, la robustesse et le respect des autres exigences pertinentes énoncées au chapitre III, section 2, ainsi que les éventuelles incidences discriminatoires; les journaux de test et tous les rapports de test datés et signés par les personnes responsables, y compris en ce qui concerne les modifications prédéterminées visées au point f);
- h) les mesures de cybersécurité qui ont été prises;

3. des informations détaillées sur la surveillance, le fonctionnement et le contrôle du système d'IA, en particulier en ce qui concerne: les capacités et les limites du système sur le plan de sa performance, y compris le degré d'exactitude pour des personnes ou des groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé et le niveau global d'exactitude prévu par rapport à sa destination; les résultats non intentionnels et sources de risques prévisibles pour la santé et la sécurité, les droits fondamentaux et en termes de discrimination compte tenu de la destination du système d'IA; les mesures de contrôle humain nécessaires conformément à l'article 14, y compris les mesures techniques mises en place pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA; les spécifications concernant les données d'entrée, le cas échéant;
4. une description de l'adéquation des indicateurs de performance à ce système d'IA spécifique;
5. une description détaillée du système de gestion des risques conformément à l'article 9;
6. une description des modifications pertinentes apportées par le fournisseur au système tout au long de son cycle de vie;
7. une liste des normes harmonisées appliquées, en totalité ou en partie, dont les références ont été publiées au *Journal officiel de l'Union européenne*; lorsqu'aucune norme harmonisée de ce type n'a été appliquée, une description détaillée des solutions adoptées pour satisfaire aux exigences énoncées au chapitre III, section 2, y compris une liste des autres normes pertinentes et spécifications techniques appliquées;
8. une copie de la déclaration UE de conformité visée à l'article 47;
9. une description détaillée du système en place pour évaluer les performances du système d'IA après la commercialisation conformément à l'article 72, y compris le plan de surveillance après commercialisation visé à l'article 72, paragraphe 3.

ANNEXE V

Déclaration UE de conformité

La déclaration UE de conformité visée à l'article 47 contient l'ensemble des informations suivantes:

1. le nom et le type du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
2. le nom et l'adresse du fournisseur ou, le cas échéant, de son mandataire;
3. une attestation certifiant que la déclaration UE de conformité visée à l'article 47 est établie sous la seule responsabilité du fournisseur;
4. une déclaration attestant que le système d'IA respecte le présent règlement et, le cas échéant, toute autre législation de l'Union applicable prévoyant l'établissement de la déclaration UE de conformité visée à l'article 47;
5. lorsqu'un système d'IA nécessite le traitement de données à caractère personnel, une déclaration qui atteste que ledit système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 ainsi qu'à la directive (UE) 2016/680;
6. des références aux éventuelles normes harmonisées pertinentes utilisées ou aux éventuelles autres spécifications communes par rapport auxquelles la conformité est déclarée;

7. le cas échéant, le nom et le numéro d'identification de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré;
 8. le lieu et la date de délivrance de la déclaration, le nom et la fonction du signataire ainsi que la mention de la personne pour le compte de laquelle ce dernier a signé, et une signature.
-

ANNEXE VI

Procédure d'évaluation de la conformité fondée sur le contrôle interne

1. La procédure d'évaluation de la conformité fondée sur le contrôle interne est la procédure d'évaluation de la conformité décrite aux points 2, 3 et 4.
 2. Le fournisseur vérifie que le système de gestion de la qualité établi est conforme aux exigences de l'article 17.
 3. Le fournisseur examine les informations contenues dans la documentation technique afin d'évaluer la conformité du système d'IA aux exigences essentielles pertinentes énoncées au chapitre III, section 2.
 4. Le fournisseur vérifie également que le processus de conception et de développement du système d'IA et son système de surveillance après commercialisation prévu à l'article 72 sont cohérents avec la documentation technique.
-

ANNEXE VII

Conformité fondée sur une évaluation du système de gestion de la qualité
et une évaluation de la documentation technique

1. Introduction

La conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique est la procédure d'évaluation de la conformité décrite aux points 2 à 5.

2. Vue d'ensemble

Le système de gestion de la qualité approuvé pour la conception, le développement et les essais des systèmes d'IA conformément à l'article 17 est examiné conformément au point 3 et soumis à la surveillance spécifiée au point 5. La documentation technique du système d'IA est examinée conformément au point 4.

3. Système de gestion de la qualité

3.1. La demande du fournisseur comprend:

- a) le nom et l'adresse du fournisseur, ainsi que le nom et l'adresse d'un mandataire si la demande est introduite par celui-ci;
- b) la liste des systèmes d'IA couverts par le même système de gestion de la qualité;
- c) la documentation technique de chaque système d'IA couvert par le même système de gestion de la qualité;

- d) la documentation relative au système de gestion de la qualité qui couvre tous les aspects énumérés à l'article 17;
- e) une description des procédures en place pour garantir que le système de gestion de la qualité reste adéquat et efficace;
- f) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié.

3.2. Le système de gestion de la qualité est évalué par l'organisme notifié, qui détermine s'il satisfait aux exigences visées à l'article 17.

La décision est notifiée au fournisseur ou à son mandataire.

La notification contient les conclusions de l'évaluation du système de gestion de la qualité et la décision d'évaluation motivée.

3.3. Le système de gestion de la qualité tel qu'approuvé continue d'être mis en œuvre et adapté par le fournisseur afin de rester adéquat et efficace.

3.4. Toute modification envisagée du système de gestion de la qualité approuvé ou de la liste des systèmes d'IA couverts par ce dernier est portée à l'attention de l'organisme notifié par le fournisseur.

Les modifications proposées sont examinées par l'organisme notifié, qui décide si le système de gestion de la qualité modifié continue de satisfaire aux exigences visées au point 3.2, ou si une réévaluation est nécessaire.

L'organisme notifié notifie sa décision au fournisseur. La notification contient les conclusions de l'examen des modifications et la décision d'évaluation motivée.

4. Contrôle de la documentation technique
- 4.1. Outre la demande visée au point 3, une demande est déposée par le fournisseur auprès d'un organisme notifié de son choix pour l'évaluation de la documentation technique relative au système d'IA que le fournisseur prévoit de mettre sur le marché ou de mettre en service et qui est couvert par le système de gestion de la qualité visé au point 3.
- 4.2. La demande comprend:
 - a) le nom et l'adresse du fournisseur;
 - b) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié;
 - c) la documentation technique visée à l'annexe IV.
- 4.3. La documentation technique est examinée par l'organisme notifié. Lorsque cela est pertinent et dans les limites de ce qui est nécessaire à l'accomplissement de ses tâches, l'organisme notifié se voit accorder un accès complet aux jeux de données d'entraînement, de validation et d'essai utilisés, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'API ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

- 4.4. Lors de l'examen de la documentation technique, l'organisme notifié peut exiger que le fournisseur apporte des preuves supplémentaires ou effectue des essais supplémentaires afin de permettre une évaluation correcte de la conformité du système d'IA avec les exigences énoncées au chapitre III, section 2. Lorsque l'organisme notifié n'est pas satisfait des essais effectués par le fournisseur, l'organisme notifié effectue directement des essais adéquats, le cas échéant.
- 4.5. Lorsque cela est nécessaire pour évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2, après que tous les autres moyens raisonnables de vérifier la conformité ont été épuisés et se sont révélés insuffisants, et sur demande motivée, l'accès aux modèles d'entraînement et aux modèles entraînés du système d'IA, y compris à ses paramètres pertinents, est aussi accordé à l'organisme notifié. Cet accès est soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires.
- 4.6. La décision de l'organisme notifié est notifiée au fournisseur ou à son mandataire. La notification contient les conclusions de l'évaluation de la documentation technique et la décision d'évaluation motivée.

Lorsque le système d'IA est conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié délivre un certificat d'évaluation UE de la documentation technique. Le certificat indique le nom et l'adresse du fournisseur, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du système d'IA.

Le certificat et ses annexes contiennent toutes les informations pertinentes pour permettre l'évaluation de la conformité du système d'IA et le contrôle du système d'IA pendant son utilisation, le cas échéant.

Lorsque le système d'IA n'est pas conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié refuse de délivrer un certificat d'évaluation UE de la documentation technique et en informe le demandeur, en lui précisant les raisons de son refus.

Lorsque le système d'IA ne satisfait pas à l'exigence relative aux données utilisées pour l'entraîner, il devra être entraîné à nouveau avant l'introduction d'une nouvelle demande d'évaluation de la conformité. Dans ce cas, la décision d'évaluation motivée de l'organisme notifié refusant de délivrer le certificat d'évaluation UE de la documentation technique contient des considérations spécifiques sur la qualité des données utilisées pour entraîner le système d'IA, en particulier sur les raisons de la non-conformité.

- 4.7. Les éventuelles modifications du système d'IA susceptibles d'avoir une incidence sur la conformité du système d'IA avec les exigences ou sur sa destination sont évaluées par l'organisme notifié qui a délivré le certificat d'évaluation UE de la documentation technique. Le fournisseur informe cet organisme notifié de son intention d'introduire une telle modification ou s'il prend autrement connaissance de l'existence de telles modifications. Les modifications envisagées sont évaluées par l'organisme notifié, qui décide si elles nécessitent une nouvelle évaluation de la conformité conformément à l'article 43, paragraphe 4, ou si elles peuvent faire l'objet d'un document complémentaire au certificat d'évaluation UE de la documentation technique. Dans ce dernier cas, l'organisme notifié évalue les modifications, informe le fournisseur de sa décision et, lorsque les modifications sont approuvées, lui fournit un document complémentaire au certificat d'évaluation UE de la documentation technique.

5. Surveillance du système de gestion de la qualité approuvé
- 5.1. Le but de la surveillance effectuée par l'organisme notifié visé au point 3 est de s'assurer que le fournisseur se conforme dûment aux conditions du système de gestion de la qualité approuvé.
- 5.2. À des fins d'évaluation, le fournisseur autorise l'organisme notifié à accéder aux locaux où les systèmes d'IA sont conçus, développés ou mis à l'essai. Le fournisseur partage en outre avec l'organisme notifié toutes les informations nécessaires.
- 5.3. L'organisme notifié effectue périodiquement des audits pour s'assurer que le fournisseur maintient et applique le système de gestion de la qualité; il transmet un rapport d'audit au fournisseur. Dans le cadre de ces audits, l'organisme notifié peut effectuer des essais supplémentaires des systèmes d'IA pour lesquels un certificat d'évaluation UE de la documentation technique a été délivré.
-

ANNEXE VIII

Informations à fournir lors de l'enregistrement d'un système d'IA à haut risque
conformément à l'article 49

Section A - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque
conformément à l'article 49, paragraphe 1

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 1:

1. le nom, l'adresse et les coordonnées du fournisseur;
2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;
3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;
4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
5. une description de la destination du système d'IA ainsi que des composants et fonctions gérées au moyen de ce système d'IA;
6. une description de base et concise des informations utilisées par le système (données, entrées) et de sa logique de fonctionnement;

7. le statut du système d'IA (sur le marché ou en service; plus mis sur le marché/en service, rappelé);
8. le type, le numéro et la date d'expiration du certificat délivré par l'organisme notifié et le nom ou le numéro d'identification de cet organisme notifié, le cas échéant;
9. une copie numérisée du certificat visé au point 8, le cas échéant;
10. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union;
11. une copie de la déclaration UE de conformité visée à l'article 47;
12. une notice d'utilisation en format électronique; ces informations ne sont pas à fournir pour les systèmes d'IA à haut risque dans les domaines des activités répressives ou de la migration, de l'asile et de la gestion des contrôles aux frontières visés à l'annexe III, points 1, 6 et 7;
13. une adresse URL vers des informations supplémentaires (facultatif).

Section B - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque
conformément à l'article 49, paragraphe 2

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à enregistrer conformément à l'article 49, paragraphe 2:

1. le nom, l'adresse et les coordonnées du fournisseur;
2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;
3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;
4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
5. une description de la destination du système d'IA;
6. la ou les conditions visées à l'article 6, paragraphe 3, sur la base desquelles le système d'IA est considéré comme n'étant pas à haut risque;
7. un résumé succinct des motifs pour lesquels le système d'IA est considéré comme n'étant pas à haut risque en application de la procédure prévue à l'article 6, paragraphe 3;
8. le statut du système d'IA (sur le marché ou en service; plus sur le marché/en service, rappelé);
9. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union.

Section C - Informations à fournir par les déployeurs de systèmes d'IA à haut risque
conformément à l'article 49, paragraphe 3

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 3:

1. le nom, l'adresse et les coordonnées du déployeur;
2. le nom, l'adresse et les coordonnées de toute personne qui soumet des informations au nom du déployeur;
3. l'adresse URL de l'entrée du système d'IA dans la base de données de l'UE par son fournisseur;
4. une synthèse des conclusions de l'analyse d'impact sur les droits fondamentaux réalisée conformément à l'article 27;
5. un résumé de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, comme précisé à l'article 26, paragraphe 8, du présent règlement, le cas échéant.

ANNEXE IX

Informations à fournir lors de l'enregistrement de systèmes d'IA à haut risque
énumérés à l'annexe III en ce qui concerne les essais en conditions réelles
conformément à l'article 60

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les essais en conditions réelles à enregistrer conformément à l'article 60:

1. un numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles;
2. le nom et les coordonnées du fournisseur ou du fournisseur potentiel et des dépoyeurs participant aux essais en conditions réelles;
3. une brève description du système d'IA et de sa destination, ainsi que d'autres informations nécessaires à l'identification du système;
4. une synthèse des caractéristiques principales du plan d'essais en conditions réelles;
5. des informations sur la suspension ou la cessation des essais en conditions réelles.

ANNEXE X

Actes législatifs de l'Union relatifs aux systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

1. Système d'information Schengen

- a) Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).
- b) Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018, p. 14).
- c) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

2. Système d'information sur les visas

- a) Règlement (UE) 2021/1133 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (UE) n° 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 et (UE) 2019/818 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système d'information sur les visas (JO L 248 du 13.7.2021, p. 1).
- b) Règlement (UE) 2021/1134 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) n° 767/2008, (CE) n° 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 et (UE) 2019/1896 du Parlement européen et du Conseil et abrogeant les décisions 2004/512/CE et 2008/633/JAI du Conseil, aux fins de réformer le système d'information sur les visas (JO L 248 du 13.7.2021, p. 11).

3. Eurodac

Règlement (UE) 2024/... du Parlement européen et du Conseil du ... relatif à la création d'"Eurodac" pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/..., (UE) 2024/... du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n° 603/2013 du Parlement européen et du Conseil⁺.

4. Système d'entrée/de sortie

Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 (JO L 327 du 9.12.2017, p. 20).

⁺ JO: veuillez insérer dans le corps du texte le numéro du règlement figurant dans le document PE-CONS 15/24 (2016/0132 (COD)) et insérer le numéro, la date, le titre et la référence au JO dudit règlement dans la note de bas de page.

5. Système européen d'information et d'autorisation concernant les voyages
- a) Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n° 1077/2011, (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1).
 - b) Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) (JO L 236 du 19.9.2018, p. 72).
6. Système européen d'information sur les casiers judiciaires concernant des ressortissants de pays tiers et des apatrides
- Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

7. Interopérabilité

- a) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI (JO L 135 du 22.5.2019, p. 27).
 - b) Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85).
-

ANNEXE XI

Documentation technique visée à l'article 53, paragraphe 1, point a)

– documentation technique pour les fournisseurs de modèles d'IA à usage général

Section 1

Informations devant être fournies

par tous les fournisseurs de modèles d'IA à usage général

La documentation technique visée à l'article 53, paragraphe 1, point a), contient au moins les informations ci-après, en fonction de la taille et du profil de risque du modèle:

1. Une description générale du modèle d'IA à usage général, y compris:
 - a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;
 - b) les politiques applicables en matière d'utilisation acceptable;
 - c) la date de publication et les méthodes de distribution;
 - d) l'architecture et le nombre de paramètres;
 - e) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;
 - f) la licence.

2. Une description détaillée des éléments du modèle visés au point 1, et des informations pertinentes sur le processus de développement, y compris les éléments suivants:
- a) les moyens techniques (p. ex.: notice d'utilisation, infrastructure, outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;
 - b) les spécifications de conception du modèle et du processus d'entraînement, y compris les méthodes et techniques d'entraînement, les principaux choix de conception, y compris le raisonnement et les hypothèses retenues; ce que le modèle est conçu pour optimiser, ainsi que la pertinence des différents paramètres, le cas échéant;
 - c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation (p. ex.: nettoyage, filtrage, etc.), le nombre de points de données, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées, ainsi que toutes les autres mesures visant à détecter l'inadéquation des sources de données et les méthodes permettant de détecter les biais identifiables, le cas échéant;
 - d) les ressources informatiques utilisées pour entraîner le modèle (p. ex.: nombre d'opérations en virgule flottante), le temps d'entraînement et d'autres détails pertinents liés à l'entraînement;
 - e) la consommation d'énergie connue ou estimée du modèle.

En ce qui concerne le point e), lorsque la consommation d'énergie du modèle est inconnue, la consommation d'énergie peut être estimée en s'appuyant sur des informations concernant les ressources informatiques utilisées.

Section 2

Informations devant être fournies

par les fournisseurs de modèles d'IA à usage général présentant un risque systémique

1. Une description détaillée des stratégies d'évaluation, y compris les résultats de l'évaluation, sur la base des protocoles et outils d'évaluation publics disponibles ou d'autres méthodes d'évaluation. Les stratégies d'évaluation comprennent des critères, des indicateurs et les méthodes d'évaluation pour l'identification des limites.
 2. Le cas échéant, une description détaillée des mesures mises en place pour effectuer des essais contradictoires internes et/ou externes (p. ex.: méthode de l'équipe rouge), des adaptations de modèles, y compris l'alignement et le réglage fin.
 3. Le cas échéant, une description détaillée de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global.
-

ANNEXE XII

Informations relatives à la transparence visées à l'article 53, paragraphe 1, point b)
– documentation technique pour les fournisseurs de modèles d'IA à usage général
aux fournisseurs en aval qui intègrent le modèle dans leur système d'IA

Les informations visées à l'article 53, paragraphe 1, point b) comprennent au moins:

1. Une description générale du modèle d'IA à usage général, y compris:
 - a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;
 - b) les politiques applicables en matière d'utilisation acceptable;
 - c) la date de publication et les méthodes de distribution;
 - d) la manière dont le modèle interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels qui ne font pas partie du modèle lui-même, le cas échéant;
 - e) les versions des logiciels pertinents liés à l'utilisation du modèle d'IA à usage général, le cas échéant;
 - f) l'architecture et le nombre de paramètres;
 - g) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;
 - h) la licence pour le modèle.

2. Une description des éléments du modèle et de son processus de développement, notamment:
- a) les moyens techniques (p. ex.: la notice d'utilisation, l'infrastructure, les outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;
 - b) les modalités (p. ex.: texte, image, etc.) et le format des entrées et des sorties, ainsi que leur taille maximale (p. ex.: taille de la fenêtre de contexte, etc.);
 - c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation.
-

ANNEXE XIII

Critères de désignation des modèles d'IA à usage général présentant un risque systémique visés à l'article 51

Aux fins de déterminer si un modèle d'IA à usage général a des capacités ou un impact équivalents à ceux énoncés à l'article 51, paragraphe 1, point a), la Commission tient compte des critères suivants:

- a) le nombre de paramètres du modèle;
- b) la qualité ou la taille du jeu de données, par exemple mesurée en tokens;
- c) la quantité de calcul utilisée pour l'entraînement du modèle, mesurée en nombre d'opérations en virgule flottante ou indiquée par une combinaison d'autres variables telles que le coût estimé de l'entraînement, le temps estimé nécessaire à l'entraînement ou la consommation d'énergie estimée pour l'entraînement;
- d) les modalités d'entrée et de sortie du modèle, telles que la conversion de texte en texte (grands modèles de langage), la conversion de texte en image, la multimodalité et les seuils de l'état de l'art pour déterminer les capacités à fort impact pour chaque modalité, ainsi que le type spécifique d'entrées et de sorties (p. ex.: séquences biologiques);
- e) les critères de référence et les évaluations des capacités du modèle, y compris en tenant compte du nombre de tâches ne nécessitant pas d'entraînement supplémentaire, sa capacité d'adaptation à apprendre de nouvelles tâches distinctes, son niveau d'autonomie et d'extensibilité, ainsi que les outils auxquels il a accès;

- f) si le modèle a un impact important sur le marché intérieur en raison de sa portée, qui est présumée lorsqu'il a été mis à la disposition d'au moins 10 000 utilisateurs professionnels enregistrés établis dans l'Union;
 - g) le nombre d'utilisateurs finaux inscrits."
-

ISPRAVAK

Uredbe (EU) Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji)

(PE-CONS 24/1/24 REV 1, 14. lipnja 2024.)

Uredba sadržana u dokumentu PE-CONS 24/1/24 REV 1 glasi kako slijedi:

**„UREDBA (EU) 2024/...
EUROPSKOG PARLAMENTA I VIJEĆA**

od 13. lipnja 2024.

**o utvrđivanju usklađenih pravila o umjetnoj inteligenciji
i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013,
(EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144
te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828
(Akt o umjetnoj inteligenciji)**

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegove članke 16. i 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrtu zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora¹,

uzimajući u obzir mišljenje Europske središnje banke²,

uzimajući u obzir mišljenje Odbora regija³,

u skladu s redovnim zakonodavnim postupkom⁴,

¹ SL C 517, 22.12.2021., str. 56.

² SL C 115, 11.3.2022., str. 5.

³ SL C 97, 28.2.2022., str. 60.

⁴ Stajalište Europskog parlamenta od 13. ožujka 2024. (još nije objavljeno u Službenom listu) i Odluka Vijeća od 21. svibnja 2024.

budući da:

- (1) Svrha je ove Uredbe poboljšati funkcioniranje unutarnjeg tržišta utvrđivanjem ujednačenog pravnog okvira, osobito za razvoj, stavljanje na tržište, stavljanje u upotrebu i korištenje sustava umjetne inteligencije („UI sustavi”) u Uniji, u skladu s vrijednostima Unije, promicati prihvaćanje antropocentrične i pouzdane umjetne inteligencije uz istodobno jamčenje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava kako su sadržana u Povelji Europske unije o temeljnim pravima („Povelja”), uključujući demokraciju, vladavinu prava i zaštitu okoliša, zaštitu od štetnih učinaka UI sustavâ u Uniji, te podupirati inovacije. Ovom se Uredbom osigurava slobodno prekogranično kretanje robe i usluga temeljenih na umjetnoj inteligenciji, čime se države članice sprečava da nametnu ograničenja razvoju, stavljanju na tržište i korištenju UI sustavâ, osim ako je to izričito odobreno ovom Uredbom.
- (2) Ova bi se Uredba trebala primjenjivati u skladu s vrijednostima Unije sadržanima u Povelji i trebala bi olakšati zaštitu fizičkih osoba, poduzeća, demokracije, vladavine prava i okoliša, a istodobno poticati inovacije i zapošljavanje te učiniti Uniju predvodnikom u prihvaćanju pouzdane umjetne inteligencije.

- (3) UI sustavi mogu se lako uvesti u brojne različite sektore gospodarstva i mnoge dijelove društva, među ostalim i preko granica, te lako cirkulirati u cijeloj Uniji. Neke su države članice već razmotrile donošenje nacionalnih pravila kojima bi se zajamčilo da umjetna inteligencija bude pouzdana i sigurna te da se razvija i upotrebljava u skladu s obvezama u području temeljnih prava. Divergentna nacionalna pravila mogu dovesti do fragmentacije unutarnjeg tržišta i smanjiti pravnu sigurnost za operatere koji razvijaju, uvoze ili upotrebljavaju UI sustave. Stoga bi za postizanje pouzdane umjetne inteligencije trebalo osigurati dosljednu i visoku razinu zaštite u cijeloj Uniji, dok bi divergencije koje otežavaju slobodnu cirkulaciju, inovacije te uvođenje i prihvaćanje UI sustava i povezanih proizvoda i usluga na unutarnjem tržištu trebalo spriječiti utvrđivanjem ujednačenih obveza za operatere i jamčenjem ujednačene zaštite prevladavajućih razloga od javnog interesa i pravâ osoba na cijelom unutarnjem tržištu na temelju članka 114. Ugovora o funkcioniranju Europske unije (UFEU). U mjeri u kojoj ova Uredba sadržava specifična pravila o zaštiti pojedinaca u pogledu obrade osobnih podataka u vezi s ograničenjima korištenja UI sustavâ za daljinsku biometrijsku identifikaciju u svrhu kaznenog progona, korištenja UI sustavâ za procjene rizika u pogledu fizičkih osoba u svrhu kaznenog progona i korištenja UI sustavâ za biometrijsku kategorizaciju u svrhu kaznenog progona, primjereno je ovu Uredbu, u mjeri u kojoj se odnosi na ta specifična pravila, temeljiti na članku 16. UFEU-a. S obzirom na ta specifična pravila i pozivanje na članak 16. UFEU-a, primjereno je zatražiti mišljenje Europskog odbora za zaštitu podataka.

- (4) Umjetna inteligencija skup je tehnologija koji se brzo razvija i doprinosi širokom spektru gospodarskih, okolišnih i društvenih koristi u cijelom nizu industrija i društvenih aktivnosti. Zahvaljujući boljem predviđanju, optimizaciji operacija i dodjeli resursa te personalizaciji digitalnih rješenja dostupnih pojedincima i organizacijama, korištenje umjetne inteligencije može poduzećima pružiti ključne konkurentske prednosti te podupirati društveno i okolišno korisne ishode, na primjer u zdravstvu, poljoprivredi, sigurnosti hrane, obrazovanju i osposobljavanju, medijima, sportu, kulturi, upravljanju infrastrukturom, energetici, prometu i logistici, javnim uslugama, sigurnosti, pravosuđu, resursnoj i energetske učinkovitosti, praćenju stanja okoliša, očuvanju i obnovi bioraznolikosti i ekosustavâ te ublažavanju klimatskih promjena i prilagodbi njima.
- (5) Istodobno, ovisno o okolnostima njezine specifične primjene, korištenja i razine tehnološkog razvoja, umjetna inteligencija može stvoriti rizike i uzrokovati štetu javnim interesima i temeljnim pravima zaštićenima pravom Unije. Ta šteta može biti materijalna ili nematerijalna, uključujući tjelesnu, psihološku, društvenu ili ekonomsku štetu.

- (6) S obzirom na velik učinak koji umjetna inteligencija može imati na društvo i potrebu za izgradnjom povjerenja, ključno je da se umjetna inteligencija i njezin regulatorni okvir razvijaju u skladu s vrijednostima Unije sadržanima u članku 2. Ugovora o Europskoj uniji (UEU), temeljnim pravima i slobodama sadržanima u Ugovorima i, na temelju članka 6. UEU-a, u Povelji. Umjetna inteligencija neophodno bi trebala biti antropocentrična tehnologija. Trebala bi služiti kao alat namijenjen ljudima s krajnjim ciljem povećanja njihove dobrobiti.
- (7) Kako bi se osigurala dosljedna i visoka razina zaštite javnih interesa u smislu zdravlja, sigurnosti i temeljnih prava, trebalo bi utvrditi zajednička pravila za visokorizične UI sustave. Ta bi pravila trebala biti dosljedna s Poveljom, nediskriminirajuća i usklađena s međunarodnim trgovinskim obvezama Unije. Njima bi se ujedno trebalo uzeti u obzir Europsku deklaraciju o digitalnim pravima i načelima za digitalno desetljeće i Etičke smjernice za pouzdanu umjetnu inteligenciju koje je sastavila Stručna skupina na visokoj razini za umjetnu inteligenciju.

- (8) Stoga je potreban pravni okvir Unije kojim se utvrđuju usklađena pravila o umjetnoj inteligenciji kako bi se poticali razvoj, korištenje i prihvaćanje umjetne inteligencije na unutarnjem tržištu i istodobno ostvarila visoka razina zaštite javnih interesa, kao što su zdravlje i sigurnost te zaštita temeljnih prava, uključujući demokraciju, vladavinu prava i zaštitu okoliša, kako su priznata i zaštićena pravom Unije. Da bi se postigao taj cilj, trebalo bi utvrditi pravila kojima se uređuju stavljanje na tržište, stavljanje u upotrebu i korištenje određenih UI sustava, te tako osigurati neometano funkcioniranje unutarnjeg tržišta i omogućiti da ti sustavi ostvaruju koristi od načela slobodnog kretanja robe i usluga pogoduju. Ta bi pravila trebala biti jasna i snažna u zaštiti temeljnih prava, podupirati nova inovativna rješenja i pogodovati europskom ekosustavu javnih i privatnih aktera koji stvaraju UI sustave u skladu s vrijednostima Unije te ostvariti potencijal digitalne transformacije u svim regijama Unije. Utvrđivanjem tih pravila i mjera za potporu inovacijama s osobitim naglaskom na malim i srednjim poduzećima (MSP-ovi), uključujući *start-up* poduzeća, ovom se Uredbom doprinosi cilju promicanja europskog antropocentričnog pristupa umjetnoj inteligenciji i globalnog vodstva u razvoju sigurne, pouzdane i etične umjetne inteligencije kako je navelo Europsko vijeće⁵ te se osigurava zaštita etičkih načela u skladu s izričitim zahtjevom Europskog parlamenta⁶.

⁵ Europsko vijeće, izvanredni sastanak Europskog vijeća (1. i 2. listopada 2020.) – zaključci, EUCO 13/20, 2020., str. 6.

⁶ Rezolucija Europskog parlamenta od 20. listopada 2020. s preporukama Komisiji o okviru etičkih aspekata umjetne inteligencije, robotike i s njima povezanih tehnologija, 2020/2012(INL).

- (9) Usklađena pravila koja se primjenjuju na stavljanje na tržište, stavljanje u upotrebu i korištenje visokorizičnih UI sustava trebala bi biti utvrđena u skladu s Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća⁷, Odlukom br. 768/2008/EZ Europskog parlamenta i Vijeća⁸ i Uredbom (EU) 2019/1020 Europskog parlamenta i Vijeća⁹ (novi zakonodavni okvir). Usklađena pravila utvrđena u ovoj Uredbi trebala bi se primjenjivati u svim sektorima i, u skladu s novim zakonodavnim okvirom, ne bi trebala dovoditi u pitanje postojeće pravo Unije, osobito ono u području zaštite podataka, zaštite potrošača, temeljnih prava, zapošljavanja, zaštite radnika i sigurnosti proizvoda, koje ova Uredba dopunjuje. Kao posljedica toga sva prava i pravna sredstva predviđena tim pravom Unije za potrošače i druge osobe na koje UI sustavi mogu imati negativan učinak, među ostalim i u pogledu naknade potencijalne štete na temelju Direktive Vijeća 85/374/EEZ¹⁰,

⁷ Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).

⁸ Odluka br. 768/2008/EZ Europskog parlamenta i Vijeća od 9. srpnja 2008. o zajedničkom okviru za stavljanje na tržište proizvoda i o stavljanju izvan snage Odluke Vijeća 93/465/EEZ (SL L 218, 13.8.2008., str. 82.).

⁹ Uredba (EU) 2019/1020 Europskog parlamenta i Vijeća od 20. lipnja 2019. o nadzoru tržišta i sukladnosti proizvoda i o izmjeni Direktive 2004/42/EZ i uredbi (EZ) br. 765/2008 i (EU) br. 305/2011 (SL L 169, 25.6.2019., str. 1.).

¹⁰ Direktiva Vijeća 85/374/EEZ od 25. srpnja 1985. o približavanju zakona i drugih propisa država članica u vezi s odgovornošću za neispravne proizvode (SL L 210, 7.8.1985., str. 29.).

i dalje su nepromijenjeni i u potpunosti se primjenjuju. Nadalje, u kontekstu zapošljavanja i zaštite radnika, ova Uredba stoga ne bi trebala utjecati na pravo Unije o socijalnoj politici i nacionalno radno pravo, u skladu s pravom Unije, koje se odnosi na zapošljavanje i radne uvjete, uključujući zdravlje i sigurnost na radu te odnos između poslodavaca i radnika. Ova Uredba ne bi trebala utjecati ni na ostvarivanje temeljnih prava priznatih u državama članicama i na razini Unije, uključujući pravo ili slobodu štrajka ili poduzimanja drugih mjera obuhvaćenih specifičnim sustavima država članica u području radnih odnosa, kao i pravo na dogovaranje, kroz pregovore, na sklapanje i provedbu kolektivnih ugovora ili na poduzimanje kolektivnih mjera u skladu s nacionalnim pravom. Ova Uredba ne bi trebala utjecati na odredbe čiji je cilj poboljšanje radnih uvjeta u radu putem platformi utvrđene u direktivi Europskog parlamenta i Vijeća o poboljšanju radnih uvjeta u radu putem platformi. Usto, cilj je ove Uredbe ojačati djelotvornost tih postojećih prava i pravnih sredstava utvrđivanjem posebnih zahtjeva i obveza, među ostalim i u pogledu transparentnosti, tehničke dokumentacije i vođenja evidencije o UI sustavima. Nadalje, obveze koje su na temelju ove Uredbe nametnute različitim operaterima uključenima u lanac vrijednosti umjetne inteligencije trebale bi se primjenjivati ne dovodeći u pitanje nacionalno pravo, u skladu s pravom Unije, koje ima učinak ograničavanja korištenja određenih UI sustava ako takvo pravo nije obuhvaćeno područjem primjene ove Uredbe ili ako se njime žele ostvariti drugi legitimni ciljevi od javnog interesa koji nisu ciljevi koji se nastoje ostvariti ovom Uredbom. Na primjer, ova Uredba ne bi trebala utjecati na nacionalno radno pravo ni na pravo o zaštiti maloljetnika, odnosno osoba mlađih od 18 godina, uzimajući u obzir Opću napomenu Ujedinjenih naroda br. 25 (2021.) o pravima djece u pogledu digitalnog okružja, u mjeri u kojoj ono nije specifično za UI sustave i njime se žele ostvariti drugi legitimni ciljevi od javnog interesa.

- (10) Temeljno pravo na zaštitu osobnih podataka osobito je zajamčeno uredbama (EU) 2016/679¹¹ i (EU) 2018/1725¹² Europskog parlamenta i Vijeća te Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća¹³. Direktivom 2002/58/EZ Europskog parlamenta i Vijeća¹⁴ dodatno se štiti privatni život i povjerljivost komunikacija, među ostalim i pružanjem uvjeta za svu pohranu osobnih i neosobnih podataka u terminalnoj opremi te pristup tim podacima s terminalne opreme. Ti su pravni akti Unije temelj za održivu i odgovornu obradu podataka, među ostalim i onda kada skupovi podataka uključuju kombinaciju osobnih i neosobnih podataka. Ovom se Uredbom ne nastoji utjecati na primjenu postojećeg prava Unije kojim se uređuje obrada osobnih podataka, uključujući zadaće i ovlasti neovisnih nadzornih tijela nadležnih za praćenje usklađenosti s tim instrumentima.

¹¹ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

¹² Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

¹³ Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL L 119, 4.5.2016., str. 89.).

¹⁴ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)(SL L 201, 31.7.2002., str. 37.).

Ona usto ne utječe na obveze dobavljača UI sustava i subjekata koji uvode te sustave u njihovu ulogu voditelja obrade podataka ili izvršitelja obrade podataka koje proizlaze iz prava Unije o zaštiti osobnih podataka ili nacionalnog prava o zaštiti osobnih podataka u mjeri u kojoj dizajniranje, razvoj ili korištenje UI sustava uključuje obradu osobnih podataka. Također je primjereno pojasniti da ispitanici i dalje uživaju sva prava i jamstva koja su im dodijeljena tim pravom Unije, među ostalim i prava povezana s isključivo automatiziranim pojedinačnim donošenjem odluka, uključujući izradu profila.

Usklađena pravila o stavljanju na tržište, stavljanju u upotrebu i korištenju UI sustava uspostavljena ovom Uredbom trebala bi olakšati djelotvornu provedbu i omogućiti ostvarivanje prava ispitanika i drugih pravnih sredstava zajamčenih na temelju prava Unije o zaštiti osobnih podataka i drugih temeljnih prava.

- (11) Ovom se Uredbom ne bi trebale dovoditi u pitanje odredbe o odgovornosti pružatelja usluga posredovanja kako su utvrđene u Uredbi (EU) 2022/2065 Europskog parlamenta i Vijeća¹⁵.

¹⁵ Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) (SL L 277, 27.10.2022., str. 1.).

- (12) Pojam „UI sustav” u ovoj bi Uredbi trebalo jasno definirati i usko ga uskladiti s radom međunarodnih organizacija koje se bave umjetnom inteligencijom kako bi se zajamčila pravna sigurnost te olakšala međunarodna konvergencija i široka prihvaćenost i pritom omogućila fleksibilnost za prilagođavanje brzom tehnološkom napretku u tom području. Nadalje, ta bi se definicija trebala temeljiti na ključnim značajkama UI sustavâ po kojima se razlikuje od jednostavnijih tradicionalnih softverskih sustava ili pristupâ programiranju te ne bi trebao obuhvaćati sustave koji se temelje na pravilima koja su definirale isključivo fizičke osobe za automatsko izvršavanje operacija. Ključna značajka UI sustava njihova je sposobnost zaključivanja. Ta sposobnost zaključivanja odnosi se na proces dobivanja izlaznih vrijednosti, kao što su predviđanja, sadržaj, preporuke ili odluke, koje mogu utjecati na fizička i virtualna okružja, te na sposobnost UI sustava da izvode modele ili algoritme, ili i modele i algoritme, iz ulaznih vrijednosti ili podataka. Tehnike koje omogućuju zaključivanje pri izgradnji UI sustava uključuju pristupe strojnog učenja koji s pomoću podataka uče kako postići određene ciljeve te pristupe temeljene na logici i znanju koji izvode zaključke iz kodiranog znanja ili simboličkog prikaza zadatka koji treba riješiti. Sposobnost UI sustava da zaključuje nadilazi osnovnu obradu podataka omogućujući učenje, rezoniranje ili modeliranje. Pojam „strojni” odnosi se na činjenicu da je rad UI sustava pogonjen strojevima.

Upućivanjem na eksplicitne ili implicitne ciljeve ističe se da UI sustavi mogu raditi u skladu s eksplicitno definiranim ciljevima ili implicitnim ciljevima. Ciljevi UI sustava mogu se u specifičnom kontekstu razlikovati od namjene UI sustava. Za potrebe ove Uredbe okruža bi trebalo razumjeti kao kontekste u kojima UI sustavi rade, a izlazne vrijednosti koje UI sustav generira odražavaju različite funkcije UI sustava i uključuju predviđanja, sadržaj, preporuke ili odluke. UI sustavi dizajnirani su tako da rade s promjenjivim razinama autonomije, što znači da imaju određeni stupanj neovisnosti djelovanja od ljudske uključenosti i sposobnosti rada bez ljudske intervencije.

Prilagodljivost koju bi UI sustav mogao pokazati nakon uvođenja odnosi se na sposobnosti samostalnog učenja, koje sustavu omogućuju da se mijenja dok je u upotrebi. UI sustavi mogu se upotrebljavati samostalno ili kao komponenta nekog proizvoda, neovisno o tome je li sustav fizički integriran u proizvod (ugrađen) ili služi funkcionalnosti proizvoda, a da nije integriran u njega (neugrađen).

- (13) Pojam „subjekt koji uvodi sustav” iz ove Uredbe trebalo bi tumačiti kao svaku fizičku ili pravnu osobu, uključujući tijelo javne vlasti, javnu agenciju ili drugo javno tijelo, koja upotrebljava UI sustav u okviru svoje nadležnosti, osim ako se UI sustav upotrebljava u osobnoj neprofesionalnoj djelatnosti. Ovisno o vrsti UI sustava, njegovo korištenje može utjecati na osobe koje nisu subjekt koji ga uvodi.
- (14) Pojam „biometrijski podaci” koji se upotrebljava u ovoj Uredbi trebalo bi tumačiti s obzirom na pojam biometrijskih podataka kako je definiran u članku 4. točki 14. Uredbe (EU) 2016/679, članku 3. točki 18. Uredbe (EU) 2018/1725 i članku 3. točki 13. Direktive (EU) 2016/680. Biometrijski podaci mogu omogućiti autentifikaciju, identifikaciju ili kategorizaciju fizičkih osoba i prepoznavanje njihovih emocija.
- (15) Pojam „biometrijska identifikacija” iz ove Uredbe trebalo bi definirati kao automatizirano prepoznavanje fizičkih, fizioloških i bihevioralnih obilježja ljudi, kao što su lice, pokreti očiju, izrazi lica, oblik tijela, glas, govor, hod, držanje, srčani ritam, krvni tlak, miris i način tipkanja, u svrhu utvrđivanja identiteta pojedinca usporedbom njegovih biometrijskih podataka s biometrijskim podacima pojedinaca pohranjenima u referentnoj bazi podataka, neovisno o tome je li dotični pojedinac dao privolu. To isključuje UI sustave namijenjene za biometrijsku provjeru, uključujući autentifikaciju, čija je jedina svrha potvrditi da je određena fizička osoba doista ona kojom se predstavlja i potvrditi identitet fizičke osobe isključivo radi pristupa usluzi, otključavanja uređaja ili sigurnog pristupa prostorijama.

- (16) Pojam „biometrijska kategorizacija” iz ove Uredbe trebalo bi definirati kao razvrstavanje fizičkih osoba u određene kategorije na temelju njihovih biometrijskih podataka.
- Te specifične kategorije mogu se odnositi na aspekte kao što su spol, dob, boja kose, boja očiju, tetovaže, značajke ponašanja ili osobnosti, jezik, vjera, pripadnost nacionalnoj manjini, spolna ili politička orijentacija. To ne uključuje sustave za biometrijsku kategorizaciju koji su isključivo pomoćni element intrinzično povezan s drugom komercijalnom uslugom, što znači da se taj element iz objektivnih tehničkih razloga ne može upotrebljavati bez glavne usluge i da integracija tog elementa ili funkcionalnosti nije sredstvo za zaobilaženje primjenjivosti pravila ove Uredbe. Na primjer, filtri za kategorizaciju značajki lica ili tijela koji se upotrebljavaju na internetskim tržištima mogli bi biti takav pomoćni element jer se mogu upotrebljavati samo u vezi s glavnom uslugom koja se sastoji od prodaje proizvoda tako što se potrošaču omogućuje da pregleda prikaz proizvoda na sebi i tako što pomaže u donošenju odluke o kupnji. Filtri koji se upotrebljavaju na internetskim društvenim mrežama i kojima se kategoriziraju značajke lica ili tijela kako bi se korisnicima omogućilo dodavanje ili izmjena slika ili videozapisa također bi se mogli smatrati pomoćnim elementom jer se takvi filtri ne mogu upotrebljavati bez glavne usluge društvenih mreža koja se sastoji od dijeljenja sadržaja na internetu.

- (17) Pojam „sustav za daljinsku biometrijsku identifikaciju” iz ove Uredbe trebalo bi definirati funkcionalno kao UI sustav namijenjen identifikaciji fizičkih osoba bez njihova aktivnog sudjelovanja, obično na daljinu, usporedbom biometrijskih podataka dotične osobe s biometrijskim podacima iz referentne baze podataka, bez obzira na specifičnu tehnologiju, specifične postupke ili specifične vrste biometrijskih podataka koji se upotrebljavaju. Takvi sustavi za daljinsku biometrijsku identifikaciju obično se upotrebljavaju za istodobno percipiranje više osoba ili njihova ponašanja kako bi se znatno olakšala identifikacija fizičkih osoba bez njihova aktivnog sudjelovanja. To isključuje UI sustave namijenjene za biometrijsku provjeru, uključujući autentifikaciju, čija je jedina svrha potvrditi da je određena fizička osoba doista ona kojom se predstavlja i potvrditi identitet fizičke osobe isključivo radi pristupa usluzi, otključavanja uređaja ili sigurnog pristupa prostorijama. To je isključenje opravdano činjenicom da će takvi sustavi vjerojatno manje utjecati na temeljna prava fizičkih osoba nego sustavi za daljinsku biometrijsku identifikaciju koji se mogu upotrebljavati za obradu biometrijskih podataka velikog broja osoba bez njihova aktivnog sudjelovanja. U slučaju sustava u stvarnom vremenu prikupljanje biometrijskih podataka, usporedba i identifikacija odvijaju se trenutačno, gotovo trenutačno ili u svakom slučaju bez znatnog vremenskog odmaka. U tom pogledu ne bi trebao postojati prostor za zaobilazanje pravila iz ove Uredbe o korištenju dotičnih UI sustava u stvarnom vremenu predviđanjem kratkih vremenskih odmaka. Sustavi u stvarnom vremenu uključuju korištenje materijala snimljenog „uživo” ili „gotovo uživo”, kao što je videozapis, zabilježenog kamerom ili drugim uređajem sa sličnom funkcijom. S druge strane, u slučaju sustava za naknadnu identifikaciju biometrijski su podaci već prethodno prikupljeni te se usporedba i identifikacija provode tek nakon znatnog vremenskog odmaka. To uključuje materijal, kao što su fotografije ili videozapisi zabilježeni nadzornim kamerama ili privatnim uređajima, snimljen prije nego što je sustav upotrijebljen za identifikaciju dotičnih fizičkih osoba.

- (18) Pojam „sustav za prepoznavanje emocija” iz ove Uredbe trebalo bi definirati kao UI sustav namijenjen prepoznavanju emocija ili namjera fizičkih osoba ili izvođenju zaključaka o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka. Taj se pojam odnosi na emocije ili namjere kao što su sreća, tuga, ljutnja, iznenađenje, gađenje, osramoćenost, uzbuđenje, sram, prijezir, zadovoljstvo i zabavljenost. Ne uključuje fizička stanja, kao što su bol ili umor, među ostalim, primjerice, sustave koji se upotrebljavaju za otkrivanje stanja umora kod profesionalnih pilota ili vozača u svrhu sprečavanja nesreća. To također ne uključuje samo otkrivanje lako vidljivih izraza, gesta ili pokreta, osim ako se upotrebljavaju za identifikaciju ili izvođenje zaključaka o emocijama. Ti izrazi mogu biti osnovni izrazi lica, kao što su namrštenost ili osmijeh, ili geste kao što su pokreti ruku ili glave, ili značajke glasa osobe, kao što su podignut glas ili šaptanje.

- (19) Za potrebe ove Uredbe pojam „javno mjesto” trebalo bi razumjeti kao svako fizičko mjesto koje je dostupno neodređenom broju fizičkih osoba, bez obzira na to je li dotično mjesto u privatnom ili javnom vlasništvu i na aktivnost za koju se to mjesto može upotrebljavati, kao što su trgovina npr. trgovine, restorani, kafići, usluge npr. banke, profesionalne aktivnosti, ugostiteljstvo, sport npr. bazeni, teretane, stadioni, prijevoz npr. autobusne i željezničke postaje, postaje podzemne željeznice, zračne luke, prijevozna sredstva, zabava npr. kina, kazališta, muzeji, koncertne i konferencijske dvorane odnosno aktivnosti u slobodno vrijeme ili druge svrhe npr. javne ceste i trgovi, parkovi, šume, igrališta. Mjesto bi trebalo klasificirati kao javno i ako, bez obzira na potencijalni kapacitet ili sigurnosna ograničenja, pristup tom mjestu podliježe određenim unaprijed utvrđenim uvjetima koje može ispuniti neodređen broj osoba, kao što su kupnja ulaznice ili prijevozne karte, prethodna registracija ili određena dob. S druge strane, mjesto se ne bi trebalo smatrati javnim ako je pristup ograničen na specifične i definirane fizičke osobe putem prava Unije ili nacionalnog prava koje je izravno povezano s javnom sigurnošću ili zaštitom odnosno putem jasnog iskaza volje osobe koja ima odgovarajuće ovlasti na tom mjestu. Sama činjenična mogućnost pristupa kao što su otključana vrata ili otvoreni ulaz u ogradi ne znači da je mjesto javno ako postoje naznake ili okolnosti koje upućuju na suprotno kao što su znakovi kojima se zabranjuje ili ograničava pristup. Poslovni prostori poduzeća i tvornica te uredi i mjesta rada kojima mogu pristupiti samo relevantni zaposlenici i pružatelji usluga nisu javna mjesta. Javna mjesta ne bi trebala uključivati zatvore ili graničnu kontrolu. Neka druga mjesta mogu se sastojati i od mjesta koja su javna mjesta i od mjesta koja to nisu, kao što je hodnik privatne stambene zgrade potreban za pristup liječničkoj ordinaciji ili zračna luka. Nisu obuhvaćeni internetski prostori jer oni nisu fizički prostori. Ipak, činjenicu je li određeno mjesto javno trebalo bi utvrditi na pojedinačnoj osnovi i pritom uzeti u obzir specifične okolnosti konkretne situacije.

- (20) Kako bi se ostvarile najveće koristi od UI sustava i istodobno zaštitila temeljna prava, zdravlje i sigurnost te omogućila demokratska kontrola, pismenost u području umjetne inteligencije trebala bi dobavljačima, subjektima koji uvode sustav i osobama na koje utječe umjetna inteligencija osigurati vladanje potrebnim pojmovima kako bi mogli donositi informirane odluke o UI sustavima. Ti se pojmovi mogu razlikovati s obzirom na relevantni kontekst i mogu uključivati razumijevanje pravilne primjene tehničkih elemenata tijekom faze razvoja UI sustava, mjera koje treba primijeniti tijekom njegova korištenja, prikladnih načina tumačenja izlaznih vrijednosti UI sustava i, u slučaju osoba na koje utječe umjetna inteligencija, znanje potrebno za razumijevanje načina na koji će odluke donesene uz pomoć umjetne inteligencije utjecati na njih. U kontekstu primjene ove Uredbe pismenost u području umjetne inteligencije trebala bi svim relevantnim akterima u vrijednosnom lancu umjetne inteligencije pružiti uvide potrebne za osiguravanje odgovarajuće usklađenosti i njezina pravilnog izvršavanja. Nadalje, široka provedba mjera pismenosti u području umjetne inteligencije i uvođenje odgovarajućih daljnjih mjera mogli bi doprinijeti poboljšanju radnih uvjeta i u konačnici podržati konsolidaciju i inovacijski put pouzdane umjetne inteligencije u Uniji. Europsko vijeće za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”) trebalo bi podupirati Komisiju u promicanju alata za pismenost u području umjetne inteligencije, javne svijesti te razumijevanja koristi, rizika, zaštitnih mjera, prava i obveza povezanih s korištenjem UI sustava. U suradnji s relevantnim dionicima Komisija i države članice trebale bi olakšati izradu dobrovoljnih kodeksa ponašanja kako bi se unaprijedila pismenost u području umjetne inteligencije među osobama koje se bave razvojem, radom i korištenjem umjetne inteligencije.

- (21) Kako bi se osigurali jednaki uvjeti i djelotvorna zaštita prava i sloboda pojedinaca u cijeloj Uniji, pravila utvrđena ovom Uredbom trebala bi se primjenjivati na dobavljače UI sustava na nediskriminirajući način, bez obzira na to imaju li poslovni nastan u Uniji ili trećoj zemlji, i na subjekte koji uvode UI sustave s poslovnim nastanom u Uniji.
- (22) Određeni bi UI sustavi s obzirom na njihov digitalni karakter trebali biti obuhvaćeni područjem primjene ove Uredbe čak i ako nisu stavljeni na tržište ni u upotrebu niti se upotrebljavaju u Uniji. To se, primjerice, odnosi na operatera s poslovnim nastanom u Uniji koji od operatera s poslovnim nastanom u trećoj zemlji naruči određene usluge povezane s aktivnošću koju obavlja UI sustav koji bi se smatrao visokorizičnim. U tim bi okolnostima UI sustav kojim se služi operater u trećoj zemlji mogao obrađivati podatke koji su zakonito prikupljeni u Uniji i preneseni iz nje te operateru ugovaratelju u Uniji dostaviti izlazne podatke UI sustava koje su rezultat te obrade, a da taj UI sustav nije stavljen ni na tržište ni u upotrebu niti se upotrebljava u Uniji. Kako bi se spriječilo zaobilaženje ove Uredbe i osigurala djelotvorna zaštita fizičkih osoba koje se nalaze u Uniji, ova bi se Uredba trebala primjenjivati i na dobavljače UI sustava i subjekte koji ih uvode koji imaju poslovni nastan u trećoj zemlji, u mjeri u kojoj se u Uniji namjeravaju upotrebljavati izlazni podaci tih sustava.

Međutim, kako bi se uzeli u obzir postojeći aranžmani i posebne potrebe za budućom suradnjom sa stranim partnerima s kojima se razmjenjuju informacije i dokazi, ova se Uredba ne bi trebala primjenjivati na tijela javne vlasti treće zemlje ni na međunarodne organizacije kada djeluju u okviru suradnje ili međunarodnih sporazuma koji su na razini Unije ili na nacionalnoj razini sklopljeni s Unijom ili državama članicama radi suradnje u područjima kaznenog progona i pravosuđa, pod uvjetom da relevantna treća zemlja ili međunarodna organizacija osigura odgovarajuće zaštitne mjere u pogledu zaštite temeljnih prava i sloboda pojedinaca. To prema potrebi može obuhvaćati aktivnosti subjekata kojima su treće zemlje povjerile izvršavanje posebnih zadaća za potporu takvoj suradnji u područjima kaznenog progona i pravosuđa. Takvi okviri za suradnju ili sporazumi uspostavljeni su bilateralno između država članica i trećih zemalja ili između Europske unije, Europolu i drugih agencija Unije te trećih zemalja i međunarodnih organizacija. Tijela nadležna za nadzor tijela kaznenog progona i pravosudnih tijela na temelju ove Uredbe trebala bi procijeniti uključuju li ti okviri za suradnju ili međunarodni sporazumi odgovarajuće zaštitne mjere u pogledu zaštite temeljnih prava i sloboda pojedinaca. Nacionalna tijela primatelji i institucije, tijela, uredi i agencije Unije koji se služe takvim izlaznim podacima u Uniji i dalje snose odgovornost za osiguravanje usklađenosti njihova korištenja s pravom Unije. Pri reviziji tih međunarodnih sporazuma ili sklapanju novih sporazuma u budućnosti ugovorne stranke trebale bi uložiti najveće moguće napore u usklađivanje tih sporazuma sa zahtjevima ove Uredbe.

- (23) Ova bi se Uredba trebala primjenjivati i na institucije, tijela, urede i agencije Unije kada djeluju kao dobavljač UI sustava ili subjekt koji ga uvodi.

- (24) Ako se i u mjeri u kojoj se UI sustavi stavljaju na tržište, stavljaju u upotrebu ili se upotrebljavaju, s izmjenama ili bez njih, u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću, te bi sustave trebalo isključiti iz područja primjene ove Uredbe neovisno o tome koja vrsta subjekta obavlja te aktivnosti, primjerice bez obzira na to radi li se o javnom ili privatnom subjektu. Kad je riječ o vojnim i obrambenim svrhama, takvo je isključenje opravdano i člankom 4. stavkom 2. UEU-a i posebnostima obrambene politike država članica i zajedničke obrambene politike Unije obuhvaćene glavom V. poglavljem 2. UEU-a koje podliježu međunarodnom javnom pravu, koje je stoga primjereniji pravni okvir za reguliranje UI sustavâ u kontekstu korištenja smrtonosne sile i drugih UI sustava u kontekstu vojnih i obrambenih aktivnosti. Kad je riječ o nacionalnoj sigurnosti, isključenje je opravdano kako činjenicom da nacionalna sigurnost ostaje isključiva odgovornost država članica, u skladu s člankom 4. stavkom 2. UEU-a, tako i posebnom prirodom i operativnim potrebama aktivnosti povezanih s nacionalnom sigurnošću i posebnim nacionalnim pravilima koja se primjenjuju na te aktivnosti. Međutim, ako se UI sustav koji je razvijen, stavljen na tržište, stavljen u upotrebu ili se njime služi u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću privremeno ili trajno upotrebljava u druge svrhe, na primjer civilne ili humanitarne, u svrhu kaznenog progona ili za potrebe javne sigurnosti, takav bi sustav bio obuhvaćen područjem primjene ove Uredbe. U tom bi slučaju subjekt koji UI sustav upotrebljava u svrhe koje nisu vojne svrhe, obrambene svrhe ili svrhe povezane s nacionalnom sigurnošću trebao osigurati usklađenost UI sustava s ovom Uredbom, osim ako je sustav s njome već usklađen. UI sustavi koji se stavljaju na tržište ili u upotrebu u isključene svrhe, odnosno vojne svrhe, obrambene svrhe ili svrhe povezane s nacionalnom sigurnošću, i u jednu ili više svrha koje nisu isključene, kao što su civilne svrhe ili kazneni progon, obuhvaćeni su područjem primjene ove Uredbe i dobavljači tih sustava trebali bi osigurati usklađenost s ovom Uredbom. U tim slučajevima činjenica da UI sustav može biti obuhvaćen područjem primjene ove Uredbe ne bi trebala utjecati na mogućnost da subjekti koji provode aktivnosti povezane s nacionalnom sigurnošću te obrambene i vojne aktivnosti, bez obzira na vrstu subjekta koji te aktivnosti obavlja, upotrebljavaju UI sustave čija je upotreba isključena iz područja primjene ove Uredbe u svrhe povezane s nacionalnom sigurnošću te vojne i obrambene svrhe. UI sustav koji se stavlja na tržište u civilne svrhe ili u svrhu kaznenog progona i koji se, s izmjenama ili bez njih, upotrebljava u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću ne bi trebao biti obuhvaćen područjem primjene ove Uredbe, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

- (25) Ovom bi se Uredbom trebale podupirati inovacije, trebala bi se poštovati sloboda znanosti te se njome ne bi smjele ugrožavati aktivnosti istraživanja i razvoja. Stoga je iz njezina područja primjene potrebno isključiti UI sustave i modele koji su posebno razvijeni i stavljeni u upotrebu isključivo u svrhu znanstvenog istraživanja i razvoja.
- Nadalje, potrebno je osigurati da ova Uredba na drugi način ne utječe na aktivnosti znanstvenog istraživanja i razvoja UI sustava ili modela prije njihova stavljanja na tržište ili u upotrebu. Kad je riječ o aktivnostima istraživanja, testiranja i razvoja u vezi s UI sustavima ili modelima usmjerenima na proizvode, odredbe ove Uredbe ne bi se trebale primjenjivati ni prije nego što se ti sustavi i modeli stave u upotrebu ili na tržište.
- Tim isključenjem ne dovodi se u pitanje obveza usklađivanja s ovom Uredbom ako se UI sustav obuhvaćen područjem primjene ove Uredbe stavlja na tržište ili u upotrebu kao rezultat takve aktivnosti istraživanja i razvoja niti se dovodi u pitanje primjena odredaba o regulatornim izoliranim okruženjima za umjetnu inteligenciju i testiranju u stvarnim uvjetima. Nadalje, ne dovodeći u pitanje isključenje UI sustava koji su posebno razvijeni i stavljeni u upotrebu isključivo u svrhu znanstvenog istraživanja i razvoja, svi ostali UI sustavi koji se mogu upotrebljavati za obavljanje bilo kakvih aktivnosti istraživanja i razvoja trebali bi i dalje podlijevati odredbama ove Uredbe. U svakom slučaju, aktivnosti istraživanja i razvoja trebale bi se provoditi u skladu s priznatim etičkim i profesionalnim standardima za znanstvena istraživanja i u skladu s primjenjivim pravom Unije.

- (26) Kako bi se uveo proporcionalan i djelotvoran skup obvezujućih pravila za UI sustave, trebalo bi slijediti jasno definiran pristup temeljen na riziku. Vrsta i sadržaj tih pravila u tom bi pristupu trebali biti primjereni intenzitetu i opsegu rizika koje mogu stvoriti UI sustavi. Stoga je potrebno zabraniti određene neprihvatljive prakse u području umjetne inteligencije te utvrditi zahtjeve za visokorizične UI sustave i obveze za relevantne operatere te obveze u pogledu transparentnosti za određene UI sustave.
- (27) Iako je pristup temeljen na riziku osnova za razmjeran i djelotvoran skup obvezujućih pravila, važno je podsjetiti na Etičke smjernice za pouzdanu umjetnu inteligenciju iz 2019. koje je izradila neovisna Stručna skupina za umjetnu inteligenciju koju je imenovala Komisija. U tim je smjernicama Stručna skupina za umjetnu inteligenciju razvila sedam neobvezujućih etičkih načela za umjetnu inteligenciju kojima se nastoji osigurati pouzdanost i etička prihvatljivost umjetne inteligencije. Tih sedam načela uključuju ljudsko djelovanje i nadzor; tehničku otpornost i sigurnost; privatnost i upravljanje podacima; transparentnost; raznolikost, nediskriminaciju i pravednost; dobrobit društva i okoliša te odgovornost. Ne dovodeći u pitanje pravno obvezujuće zahtjeve iz ove Uredbe i bilo koje drugo primjenjivo pravo Unije, te smjernice doprinose dizajniranju koherentne, pouzdane i antropocentrične umjetne inteligencije, u skladu s Poveljom i vrijednostima na kojima se Unija temelji. Prema smjernicama Stručne skupine za umjetnu inteligenciju, „ljudsko djelovanje i nadzor” znači da se UI sustavi razvijaju i upotrebljavaju kao alat koji služi ljudima, poštuje ljudsko dostojanstvo i osobnu autonomiju te funkcionira na način koji ljudi mogu na odgovarajući način kontrolirati i nadzirati.

Tehnička otpornost i sigurnost znači da se UI sustavi razvijaju i upotrebljavaju na način kojim se omogućuje otpornost u slučaju problema i odupiranje pokušajima promjene korištenja ili učinkovitosti UI sustava s ciljem da se trećim stranama omogući nezakonita upotreba, te kojim se nenamjerna šteta svodi na najmanju moguću mjeru. Privatnost i upravljanje podacima znači da se UI sustavi razvijaju i upotrebljavaju u skladu s pravilima o privatnosti i zaštiti podataka, pri čemu se obrađuju podaci koji ispunjavaju visoke standarde u pogledu kvalitete i cjelovitosti. Transparentnost znači da se UI sustavi razvijaju i upotrebljavaju na način kojim se omogućuje odgovarajuća sljedivost i objašnjivost, uz istodobno informiranje ljudi o tome da komuniciraju ili su u interakciji s UI sustavom te propisno obavješćivanje subjekata koji uvode sustav o sposobnostima i ograničenjima tog UI sustava, a osoba na koje utječe UI sustav o njihovim pravima. Raznolikost, nediskriminacija i pravednost znači da se UI sustavi razvijaju i upotrebljavaju na način koji uključuje različite aktere i kojim se promiču jednak pristup, rodna ravnopravnost i kulturna raznolikost, pri čemu se izbjegavaju diskriminirajući učinci i nepravedne pristranosti koji su zabranjeni pravom Unije ili nacionalnim pravom. Dobrobit društva i okoliša znači da se UI sustavi razvijaju i upotrebljavaju na održiv i okolišno prihvatljiv način i u korist svih ljudi, uz istodobno praćenje i procjenu dugoročnih učinaka na pojedinca, društvo i demokraciju. Ta bi se načela trebala primjenjivati i pri dizajniranju i korištenju UI modela, kada je to moguće. Ona bi u svakom slučaju trebala služiti kao osnova za izradu kodeksa ponašanja na temelju ove Uredbe. Sve dionike, uključujući industriju, akademsku zajednicu, civilno društvo i organizacije za normizaciju, potiče se da prema potrebi uzmu u obzir etička načela za razvoj dobrovoljnih najboljih praksi i normi.

- (28) Osim brojnih korisnih primjena umjetne inteligencije, ona se može i zloupotrijebiti te omogućiti nove i moćne alate za manipulativne i izrabljivačke prakse te prakse društvene kontrole. Takve su prakse osobito štetne i predstavljaju zlouporabu te bi ih trebalo zabraniti jer su protivne Unijanim vrijednostima poštovanja ljudskog dostojanstva, slobode, ravnopravnosti, demokracije i vladavine prava te temeljnih prava sadržanih u Povelji, uključujući pravo na nediskriminaciju, zaštitu podataka i privatnost te prava djeteta.

- (29) Manipulativne tehnike omogućene umjetnom inteligencijom mogu se upotrebljavati kako bi se osobe navelo na neželjeno ponašanje ili kako bi ih se obmanulo tako da ih se potiče na odluke na način kojim se podriiva i narušava njihova autonomija, donošenje odluka i slobodan izbor. Stavljanje na tržište, stavljanje u upotrebu ili korištenje određenih UI sustava s ciljem ili učinkom bitnog iskrivljavanja ljudskog ponašanja, pri čemu je vjerojatno da će nastati znatna šteta, osobito ona koja ima dovoljno velike štetne učinke na fizičko ili psihološko zdravlje odnosno financijske interese, osobito su opasni te bi ih stoga trebalo zabraniti. U takvim se UI sustavima upotrebljavaju subliminalne komponente kao što su zvučni i slikovni podražaji te videopodražaji koje osobe ne mogu percipirati jer nadilaze ljudsku percepciju ili se upotrebljavaju druge manipulativne ili prijevarne tehnike kojima se podriiva ili narušava autonomija, donošenje odluka ili slobodan izbor osobe na način da ljudi svjesno ne percipiraju te tehnike ili zbog kojih su, ako ih i jesu svjesni, svejedno prevareni ili ih ne mogu kontrolirati niti im se oduprijeti. To bi se, na primjer, moglo olakšati sučeljima mozak-računalo ili virtualnom stvarnošću jer se njima omogućuje viši stupanj kontrole toga koji se podražaji prikazuju osobama, u mjeri u kojoj bi oni mogli bitno iskriviti njihovo ponašanje na znatno štetan način. Osim toga, UI sustavi mogu na drugi način iskorištavati ranjivosti osobe ili određene skupine osoba zbog njihove dobi, invaliditeta u smislu Direktive (EU) 2019/882 Europskog parlamenta i Vijeća¹⁶ ili određene socijalne ili gospodarske situacije zbog kojih bi te osobe mogle biti izloženije iskorištavanju, kao što su osobe koje žive u ekstremnom siromaštvu i etničke ili vjerske manjine.

¹⁶ Direktiva (EU) 2019/882 Europskog parlamenta i Vijeća od 17. travnja 2019. o zahtjevima za pristupačnost proizvoda i usluga (SL L 151, 7.6.2019., str. 70.).

Takvi UI sustavi mogu se staviti na tržište, staviti u upotrebu ili se upotrebljavati s ciljem ili učinkom bitnog iskrivljavanja ponašanja osobe i to na način kojim se toj osobi ili drugoj osobi ili skupinama osoba uzrokuje znatan šteta ili je se može razumno očekivati da će se prouzročiti takva šteta, što uključuje štetu koja se može akumulirati s vremenom, te bi ih stoga trebalo zabraniti. Možda nije moguće pretpostaviti postojanje namjere da se iskrivi ponašanje ako je to iskrivljavanje ponašanja posljedica čimbenika izvan UI sustava koji su izvan kontrole dobavljača ili subjekta koji uvodi sustav, odnosno čimbenika koje dobavljač UI sustava ili subjekt koji ga uvodi ne mogu u razumnoj mjeri predvidjeti i stoga ublažiti. U svakom slučaju, nije potrebno da dobavljač UI sustava ili subjekt koji ga uvodi ima namjeru prouzročiti znatnu štetu pod uvjetom da ta šteta proizlazi iz manipulativne ili izrabljivačke prakse omogućene umjetnom inteligencijom. Zabrane takvih praksi u području umjetne inteligencije komplementarne su odredbama sadržanima u Direktivi 2005/29/EZ Europskog parlamenta i Vijeća¹⁷, osobito u pogledu toga da su nepoštene poslovne prakse koje dovode do gospodarske ili financijske štete potrošačima zabranjene u svim okolnostima, bez obzira na to provode li se putem UI sustavâ ili na drugi način. Zabrane manipulativnih i izrabljivačkih praksi iz ove Uredbe ne bi trebale utjecati na zakonite prakse u kontekstu liječenja, kao što je psihološko liječenje mentalnih bolesti ili fizička rehabilitacija, ako se te prakse provode u skladu s primjenjivim pravom i medicinskim standardima, kao što su izričita privola pojedinaca ili njihovih zakonskih zastupnika. Osim toga, uobičajene i zakonite poslovne prakse, primjerice u području oglašavanja, koje su u skladu s primjenjivim pravom ne bi same po sebi trebalo smatrati štetnom manipulativnom praksom omogućenom umjetnom inteligencijom.

¹⁷ Direktiva 2005/29/EZ Europskog parlamenta i Vijeća od 11. svibnja 2005. o nepoštenoj poslovnoj praksi poslovnog subjekta u odnosu prema potrošaču na unutarnjem tržištu i o izmjeni Direktive Vijeća 84/450/EEZ, direktiva 97/7/EZ, 98/27/EZ i 2002/65/EZ Europskog parlamenta i Vijeća, kao i Uredbe (EZ) br. 2006/2004 Europskog parlamenta i Vijeća („Direktiva o nepoštenoj poslovnoj praksi”) (SL L 149, 11.6.2005., str. 22.).

- (30) Trebalo bi zabraniti sustave biometrijske kategorizacije koji se temelje na biometrijskim podacima fizičkih osoba, kao što su lice ili otisak prstiju pojedinca, kako bi se deduciralo ili izvelo zaključke o njegovim političkim mišljenjima, članstvu u sindikatima, vjerskim ili filozofskim uvjerenjima, rasi, spolnom životu ili seksualnoj orijentaciji. Ta zabrana ne bi trebala obuhvaćati zakonito označivanje, filtriranje ili kategorizaciju skupova biometrijskih podataka prikupljenih u skladu s pravom Unije ili nacionalnim pravom na temelju biometrijskih podataka, kao što je razvrstavanje slika prema boji kose ili boji očiju, koji se, primjerice, mogu upotrebljavati u području kaznenog progona.
- (31) UI sustavi koji omogućuju društveno vrednovanje fizičkih osoba koje upotrebljavaju javni ili privatni akteri mogu rezultirati diskriminatornim ishodima i isključivanjem određenih skupina. Njima se može prekršiti pravo na dostojanstvo i nediskriminaciju te vrijednosti kao što su ravnopravnost i pravda. Takvi UI sustavi evaluiraju ili klasificiraju fizičke osobe ili skupine fizičkih osoba na temelju višestrukih podataka povezanih s njihovim društvenim ponašanjem u višestrukim kontekstima ili poznatih, izvedenih ili predviđenih osobnih značajki ili značajki osobnosti tijekom određenih razdoblja. Društveni rejting dobiven takvim UI sustavima može rezultirati štetnim ili nepovoljnim tretmanom fizičkih osoba ili cijelih skupina fizičkih osoba u društvenim kontekstima koji nisu povezani s kontekstom u kojima su podaci izvorno generirani ili prikupljeni odnosno štetnim tretmanom koji je nerazmjeran ili neopravdan u odnosu na težinu posljedica njihova društvenog ponašanja. Stoga bi UI sustave koji uključuju takve neprihvatljive prakse vrednovanja i koji rezultiraju takvim štetnim ili nepovoljnim ishodima trebalo zabraniti. Ta zabrana ne bi trebala utjecati na zakonite prakse evaluacije fizičkih osoba koje se provode u specifičnu svrhu u skladu s pravom Unije i nacionalnim pravom.

- (32) Korištenje UI sustava za daljinsku biometrijsku identifikaciju fizičkih osoba u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona osobito je intruzivno za prava i slobode dotičnih osoba, u onoj mjeri u kojoj može utjecati na privatni život velikog dijela stanovništva, pobuditi doživljaj stalnog nadzora i neizravno odvratiti od ostvarivanja slobode okupljanja i drugih temeljnih prava. Tehničke netočnosti UI sustava namijenjenih daljinskoj biometrijskoj identifikaciji fizičkih osoba mogu rezultirati pristranim rezultatima i imati diskriminacijske učinke. Takvi potencijalni pristrani rezultati i diskriminacijski učinci osobito su relevantni s obzirom na dob, etničku pripadnost, rasu, spol ili invaliditet. Osim toga, neposrednost učinka i ograničene mogućnosti za dodatne provjere ili ispravke u pogledu korištenja takvih sustava koji funkcioniraju u stvarnom vremenu nose povećane rizike za prava i slobode dotičnih osoba u kontekstu aktivnosti kaznenog progona ili na koje aktivnosti kaznenog progona utječu.

- (33) Stoga bi trebalo zabraniti korištenje tih sustava u svrhu kaznenog progona, osim u taksativno popisanim i usko definiranim situacijama u kojima je ono nužno za ostvarenje znatnog javnog interesa, čija važnost premašuje rizike. Te situacije uključuju potragu za određenim žrtvama kaznenih djela, uključujući nestale osobe, određene prijetnje životu ili tjelesnoj sigurnosti fizičkih osoba ili prijetnje od terorističkih napada i lociranje ili identifikaciju počinitelja kaznenih djela ili osumnjičenika za kaznena djela iz priloga ovoj Uredbi, ako je za ta kaznena djela u dotičnoj državi članici zapriječena kazna zatvora ili oduzimanja slobode u maksimalnom trajanju od najmanje četiri godine i kako su definirana u pravu te države članice. Takvim pragom za kaznu zatvora ili oduzimanje slobode u skladu s nacionalnim pravom doprinosi se osiguravanju toga da kazneno djelo bude dovoljno teško da bi se moglo opravdati korištenje sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu. Nadalje, popis kaznenih djela naveden u prilogu ovoj Uredbi temelji se na 32 kaznena djela navedena u Okvirnoj odluci Vijeća 2002/584/PUP¹⁸, uzimajući u obzir da su neka od tih kaznenih djela u praksi vjerojatno relevantnija od drugih, u smislu da bi primjena daljinske biometrijske identifikacije u stvarnom vremenu mogla biti predvidljivo potrebna i proporcionalna u vrlo promjenjivim opsezima za praktičnu provedbu lokalizacije ili identifikacije počinitelja različitih navedenih kaznenih djela ili osumnjičenika za ta kaznena djela i s obzirom na vjerojatne razlike u težini, vjerojatnosti i razmjeru štete ili mogućih negativnih posljedica.

¹⁸ Okvirna odluka Vijeća 2002/584/PUP od 13. lipnja 2002. o Europskom uhidbenom nalogu i postupcima predaje između država članica (SL L 190, 18.7.2002., str. 1.).

Izravna prijetnja životu ili tjelesnoj sigurnosti fizičkih osoba mogla bi također rezultirati iz ozbiljnog poremećaja kritične infrastrukture, kako je definirana u članku 2. točki 4. Direktive (EU) 2022/2557 Europskog parlamenta i Vijeća¹⁹, ako bi poremećaj u radu ili uništenje takve kritične infrastrukture prouzročili izravnu prijetnju životu ili tjelesnoj sigurnosti osobe, među ostalim i putem teške štete pružanju osnovne opskrbe stanovništva ili izvršavanju temeljne funkcije države. Osim toga, ovom bi se Uredbom trebala očuvati sposobnost tijela kaznenog progona, tijela nadležnih za nadzor granica, tijela nadležnih za imigraciju ili tijela nadležnih za azil da provode provjere identiteta u prisutnosti dotične osobe, u skladu s uvjetima utvrđenima za takve provjere u pravu Unije i nacionalnom pravu. Tijela kaznenog progona, tijela nadležna za nadzor granica, tijela nadležna za imigraciju ili tijela nadležna za azil osobito bi se trebala moći koristiti informacijskim sustavima, u skladu s pravom Unije ili nacionalnim pravom, za identifikaciju osoba koje se tijekom provjere identiteta odbijaju identificirati ili nisu u stanju navesti ili dokazati svoj identitet, a da pritom ne moraju pribaviti prethodno odobrenje na temelju ove Uredbe. To bi, na primjer, mogla biti osoba uključena u kazneno djelo, koja nije voljna ili koja zbog nesreće ili zdravstvenog stanja nije u stanju otkriti svoj identitet tijelima kaznenog progona.

¹⁹ Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (SL L 333, 27.12.2022., str. 164.).

- (34) Kako bi se osiguralo odgovorno i proporcionalno korištenje tih sustava, važno je i utvrditi da bi u svakoj od tih taksativno popisanih i usko definiranih situacija trebalo uzeti u obzir određene elemente, osobito u pogledu prirode situacije zbog koje se zahtijeva njihova upotreba i posljedica te upotrebe za prava i slobode svih dotičnih osoba te u pogledu zaštitnih mjera i uvjeta propisanih za tu upotrebu. Osim toga, sustavi za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona trebali bi se upotrebljavati samo za potvrđivanje identiteta konkretno ciljanog pojedinca i ta bi upotreba trebala biti ograničena na ono što je nužno kad je riječ o razdoblju te zemljopisnom i personalnom području primjene, uzimajući osobito u obzir dokaze ili naznake u vezi s prijetnjama, žrtvama ili počiniteljem. Upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima trebalo bi odobriti samo ako je relevantno tijelo kaznenog progona dovršilo procjenu učinka na temeljna prava i, osim ako je drukčije predviđeno u ovoj Uredbi, registriralo sustav u bazi podataka kako je utvrđeno u ovoj Uredbi. Referentna baza podataka osoba trebala bi biti primjerena za svaki slučaj korištenja u svakoj od gore navedenih situacija.

- (35) Uvjet za svaku upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona trebalo bi biti izričito i specifično odobrenje pravosudnog tijela ili neovisnog upravnog tijela države članice čija je odluka obvezujuća. Takvo bi odobrenje u načelu trebalo pribaviti prije upotrebe UI sustava radi identifikacije jedne ili više osoba. Iznimke od tog pravila trebalo bi dopustiti u propisno opravdanim situacijama na temelju hitnosti, odnosno u situacijama u kojima je potreba za upotrebom dotičnih sustava takva da je praktično i objektivno nemoguće pribaviti odobrenje prije početka upotrebe UI sustava. U takvim hitnim situacijama upotreba UI sustava trebala bi biti ograničena na apsolutno nužni minimum te podlijeći odgovarajućim zaštitnim mjerama i uvjetima, kako je utvrđeno u nacionalnom pravu i kako je odredilo samo tijelo kaznenog progona u kontekstu svakog pojedinačnog hitnog slučaja upotrebe. Osim toga, tijelo kaznenog progona trebalo bi u takvim situacijama zatražiti takvo odobrenje uz navođenje razloga zbog kojih ga nije moglo zatražiti ranije, bez nepotrebne odgode, a najkasnije u roku od 24 sata. Ako je takvo odobrenje odbijeno, upotrebu sustava za biometrijsku identifikaciju u stvarnom vremenu povezanu s tim odobrenjem trebalo bi smjesta zaustaviti te bi sve podatke povezane s takvom upotrebom trebalo odbaciti i izbrisati. Takvi podaci uključuju ulazne podatke koje je UI sustav izravno prikupio tijekom upotrebe takvog sustava te rezultate i izlazne podatke upotrebe povezane s tim odobrenjem. Ne bi trebali uključivati ulazne podatke koji su zakonito pribavljeni u skladu s drugim pravom Unije ili nacionalnim pravom. U svakom slučaju, odluku koja proizvodi negativan pravni učinak na osobu ne bi trebalo donijeti isključivo na temelju izlaznih podataka sustava za daljinsku biometrijsku identifikaciju.

- (36) Kako bi obavljali svoje zadaće u skladu sa zahtjevima utvrđenima u ovoj Uredbi i nacionalnim pravilima, relevantno tijelo za nadzor tržišta i nacionalno tijelo za zaštitu podataka trebali bi biti obaviješteni o svakom korištenju sustava za biometrijsku identifikaciju u stvarnom vremenu. Tijela za nadzor tržišta i prijavljena nacionalna tijela za zaštitu podataka trebala bi Komisiji podnositi godišnje izvješće o korištenju sustava za biometrijsku identifikaciju u stvarnom vremenu.
- (37) Nadalje, primjereno je u kontekstu iscrpnog okvira utvrđenog ovom Uredbom predvidjeti da bi takvo korištenje na državnom području države članice u skladu s ovom Uredbom trebalo biti moguće samo ako i u mjeri u kojoj je dotična država članica odlučila izričito predvidjeti mogućnost odobravanja takvog korištenja u svojim detaljnim pravilima nacionalnog prava. Stoga države članice na temelju ove Uredbe i dalje mogu slobodno odlučiti da neće uopće predvidjeti takvu mogućnost ili mogu predvidjeti takvu mogućnost samo u odnosu na neke od ciljeva kojima se može opravdati odobreno korištenje utvrđeno u ovoj Uredbi. O takvim nacionalnim pravilima trebalo bi obavijestiti Komisiju u roku od 30 dana od njihova donošenja.

- (38) Korištenje UI sustavâ za daljinsku biometrijsku identifikaciju pojedinaca u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona nužno uključuje obradu biometrijskih podataka. Pravila iz ove Uredbe kojima se, podložno određenim iznimkama, zabranjuje takvo korištenje, koja se temelje na članku 16. UFEU-a, trebala bi se primjenjivati kao *lex specialis* u odnosu na pravila o obradi biometrijskih podataka iz članka 10. Direktive (EU) 2016/680, čime se na iscrpan način uređuje takvo korištenje i obrada biometrijskih podataka. Stoga bi takvo korištenje i obrada trebali biti mogući samo u onoj mjeri u kojoj su u skladu s okvirom utvrđenim ovom Uredbom, pri čemu ne bi trebao postojati prostor, izvan tog okvira, da nadležna tijela koja djeluju u svrhu kaznenog progona upotrebljavaju takve sustave i obrađuju takve povezane podatke na temelju razloga navedenih u članku 10. Direktive (EU) 2016/680. U tom kontekstu svrha ove Uredbe nije pružanje pravne osnove za obradu osobnih podataka na temelju članka 8. Direktive (EU) 2016/680. Međutim, korištenje sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u druge svrhe osim kaznenog progona, među ostalim kad ih upotrebljavaju nadležna tijela, ne bi trebalo biti obuhvaćeno posebnim okvirom o takvom korištenju u svrhu kaznenog progona utvrđenim ovom Uredbom. Takvo korištenje u druge svrhe osim kaznenog progona stoga ne bi trebalo podlijezati zahtjevu za odobrenje na temelju ove Uredbe te važećim detaljnim pravilima nacionalnog prava kojima se daje učinak tom odobrenju.

- (39) Svaka obrada biometrijskih podataka i drugih osobnih podataka povezana s korištenjem UI sustavâ za biometrijsku identifikaciju, osim obrade povezane s korištenjem sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona kako je uređeno ovom Uredbom, i dalje bi trebala ispunjavati sve zahtjeve koji proizlaze iz članka 10. Direktive (EU) 2016/680. U svrhe koje nisu kazneni progon, člankom 9. stavkom 1. Uredbe (EU) 2016/679 i člankom 10. stavkom 1. Uredbe (EU) 2018/1725 zabranjuje se obrada biometrijskih podataka koji podliježu ograničenim iznimkama kako je predviđeno u tim člancima. Primjenom članka 9. stavka 1. Uredbe (EU) 2016/679 nacionalna tijela za zaštitu podataka već su donijela odluke o zabrani upotrebe daljinske biometrijske identifikacije u svrhe koje nisu kazneni progon.

- (40) U skladu s člankom 6.a Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, priloženog UEU-u i UFEU-u, Irsku ne obvezuju pravila utvrđena u članku 5. stavku 1. prvom podstavku točki (g), u mjeri u kojoj se primjenjuje na korištenje sustavâ biometrijske kategorizacije za aktivnosti u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, u članku 5. stavku 1. prvom podstavku točki (d), u mjeri u kojoj se primjenjuje na korištenje UI sustava obuhvaćenih tom odredbom, u članku 5. stavku 1. prvom podstavku točki (h), u članku 5. stavcima od 2. do 6. i u članku 26. stavku 10. ove Uredbe, donesena na temelju članka 16. UFEU-a, koja se odnose na obradu osobnih podataka koju vrše države članice pri obavljanju aktivnosti koje su obuhvaćene dijelom trećim glavom V. poglavljem 4. ili poglavljem 5. UFEU-a ako Irsku ne obvezuju pravila koja uređuju oblike pravosudne suradnje u kaznenim stvarima ili policijske suradnje za koja se zahtijeva usklađenost s odredbama utvrđenima na temelju članka 16. UFEU-a.

- (41) U skladu s člancima 2. i 2.a Protokola br. 22 o stajalištu Danske, priloženog UEU-u i UFEU-u, Dansku ne obvezuju pravila utvrđena u članku 5. stavku 1. točki (g), u mjeri u kojoj se primjenjuje na korištenje sustavâ biometrijske kategorizacije za aktivnosti u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, u članku 5. stavku 1. prvom podstavku točki (d), u mjeri u kojoj se primjenjuju na korištenje UI sustava obuhvaćenih tom odredbom, u članku 5. stavku 1. prvom podstavku točki (h), u članku 5. prvom podstavku stavcima od 2. do 6. i u članku 26. stavku 10. ove Uredbe, donesena na temelju članka 16. UFEU-a, niti ona podliježe primjeni tih pravila koja se odnose na obradu osobnih podataka koju vrše države članice pri obavljanju aktivnosti koje su obuhvaćene dijelom trećim glavom V. poglavljem 4. ili poglavljem 5. UFEU-a.

- (42) U skladu s pretpostavkom nedužnosti, fizičke osobe u Uniji uvijek bi trebalo prosuđivati na temelju njihova stvarnog ponašanja. Fizičke osobe nikada ne se bi trebale prosuđivati na temelju ponašanja koje je umjetna inteligencija predvidjela isključivo na temelju njihova profiliranja, obilježja osobnosti ili značajki kao što su državljanstvo, mjesto rođenja, mjesto boravišta, broj djece, razina duga ili vrsta automobila, bez opravdane sumnje da je ta osoba uključena u kriminalnu aktivnost na temelju objektivnih provjerljivih činjenica i bez ljudske procjene tih činjenica. Stoga bi trebalo zabraniti procjene rizika u pogledu fizičkih osoba u svrhu procjene vjerojatnosti da će počiniti kaznena djela ili u svrhu predviđanja počinjenja stvarnog ili potencijalnog kaznenog djela isključivo na temelju profiliranja tih osoba ili procjene njihovih obilježja osobnosti i značajki. U svakom slučaju, ta se zabrana ne odnosi niti se dotiče analitike rizika koja se ne temelji na profiliranju pojedinaca ili na obilježjima osobnosti i značajkama pojedinaca, kao što su UI sustavi koji upotrebljavaju analitiku rizika u svrhu procjene vjerojatnosti počinjenja financijskih prijevara od strane poduzeća na temelju sumnjivih transakcija ili alate za analizu rizika kako bi predvidjeli vjerojatnost lokalizacije narkotika ili nezakonite robe od strane carinskih tijela, primjerice na temelju poznatih krijumčarskih ruta.
- (43) Trebalo bi zabraniti stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava koji stvaraju ili proširuju baze podataka za prepoznavanje lica neciljanim prikupljanjem prikaza lica s interneta ili iz snimaka CCTV-a jer ta praksa doprinosi osjećaju masovnog nadzora i može dovesti do teških kršenja temeljnih prava, uključujući pravo na privatnost.

- (44) Postoji ozbiljna zabrinutost u pogledu znanstvene osnove UI sustavâ čiji je cilj utvrđivanje emocija ili izvođenje zaključaka o njima, osobito s obzirom na to da se izražavanje emocija znatno razlikuje među kulturama i situacijama, pa čak kod istog pojedinca. Među ključnim su nedostacima takvih sustava ograničena pouzdanost, nedostatak specifičnosti i ograničena mogućnost generalizacije. Stoga UI sustavi koji identificiraju emocije ili namjere fizičkih osoba ili izvode zaključke o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka mogu dovesti do diskriminatornih ishoda te biti intruzivni za prava i slobode dotičnih osoba. S obzirom na neravnotežu moći u kontekstu rada ili obrazovanja, u kombinaciji s intruzivnom prirodom tih sustava, takvi bi sustavi mogli dovesti do štetnog ili nepovoljnog tretmana određenih fizičkih osoba ili cijelih skupina određenih fizičkih osoba. Stoga bi trebalo zabraniti stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava namijenjenih za otkrivanje emocionalnog stanja pojedinaca u situacijama povezanim s radnim mjestom i obrazovanjem. Ta zabrana ne bi trebala obuhvaćati UI sustave koji se stavljaju na tržište isključivo iz medicinskih ili sigurnosnih razloga, kao što su sustavi namijenjeni terapijskoj upotrebi.
- (45) Ova Uredba ne bi trebala utjecati na prakse koje su zabranjene pravom Unije, među ostalim u okviru prava o zaštiti podataka, nediskriminacijskog prava, prava o zaštiti potrošača i prava tržišnog natjecanja.

- (46) Visokorizični UI sustavi trebali bi se stavljati na tržište Unije ili u upotrebu odnosno upotrebljavati se samo ako ispunjavaju određene obvezne zahtjeve. Tim bi se zahtjevima trebalo osigurati da visokorizični UI sustavi koji su dostupni u Uniji ili čije se izlazne vrijednosti na drugi način upotrebljavaju u Uniji ne predstavljaju neprihvatljiv rizik za važne javne interese Unije koji su priznati i zaštićeni pravom Unije. Na temelju novog zakonodavnog okvira, kako je pojašnjeno u obavijesti Komisije pod nazivom „Plavi vodič’ o provedbi pravila EU-a o proizvodima 2022.”²⁰, opće je pravilo da se više od jednog pravnog akta zakonodavstva Unije o usklađivanju, kao što su uredbe (EU) 2017/745²¹ i (EU) 2017/746²² Europskog parlamenta i Vijeća ili Direktiva 2006/42/EZ Europskog parlamenta i Vijeća²³, može primjenjivati na jedan proizvod jer se stavljanje na raspolaganje ili u upotrebu može provesti samo ako je proizvod u skladu sa svim primjenjivim zakonodavstvom Unije o usklađivanju. Kako bi se osigurala dosljednost i izbjegla nepotrebna administrativna opterećenja ili troškovi, dobavljači proizvoda koji sadržava jedan ili više visokorizičnih UI sustava, na koje se primjenjuju zahtjevi iz ove Uredbe i zahtjevi iz zakonodavstva Unije o usklađivanju navedeni u prilogu ovoj Uredbi, trebali bi biti fleksibilni u pogledu operativnih odluka o tome kako na najbolji način osigurati usklađenost proizvoda koji sadržava jedan ili više UI sustava sa svim primjenjivim zahtjevima zakonodavstva Unije o usklađivanju. UI sustavi utvrđeni kao visokorizični trebali bi biti ograničeni samo na one koji imaju znatan štetan učinak na zdravlje, sigurnost i temeljna prava osoba u Uniji i takvim bi se ograničenjem trebalo svesti na najmanju moguću mjeru bilo kakvo potencijalno ograničenje u pogledu međunarodne trgovine.

²⁰ SL C 247, 29.6.2022., str. 1.

²¹ Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1.).

²² Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176.).

²³ Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima o izmjeni Direktive 95/16/EZ (SL L 157, 9.6.2006., str. 24.).

- (47) UI sustavi mogli bi nepovoljno utjecati na zdravlje i sigurnost osoba, osobito ako ti sustavi funkcioniraju kao sigurnosne komponente proizvoda. U skladu s ciljevima zakonodavstva Unije o usklađivanju, kako bi se olakšalo slobodno kretanje proizvoda na unutarnjem tržištu i kako bi se zajamčilo da na tržište dolaze samo sigurni i sukladni proizvodi, važno je da se propisno spriječe i ublaže mogući sigurnosni rizici koje proizvod u cijelosti može predstavljati zbog svojih digitalnih komponenti, uključujući UI sustave. Na primjer, sve autonomniji roboti, bilo u kontekstu proizvodnje ili osobne skrbi i njege, trebali bi moći funkcionirati na siguran način i obavljati svoje zadaće u složenim okružjima. Slično tome, u zdravstvenom sektoru u kojem su rizici za život i zdravlje osobito visoki, sve sofisticiraniji dijagnostički sustavi i sustavi koji pomažu ljudima u donošenju odluka trebali bi biti pouzdani i točni.

- (48) Razmjer nepovoljnih učinaka UI sustava na temeljna prava zaštićena Poveljom posebno je važan pri klasificiranju UI sustava kao visokorizičnog. Ta prava uključuju pravo na ljudsko dostojanstvo, poštovanje privatnog i obiteljskog života, zaštitu osobnih podataka, slobodu izražavanja i informiranja, slobodu okupljanja i udruživanja, pravo na nediskriminaciju, pravo na obrazovanje, zaštitu potrošača, prava radnika, prava osoba s invaliditetom, rodnu ravnopravnost, prava intelektualnog vlasništva, pravo na djelotvoran pravni lijek i na pošteno suđenje, pravo na obranu i pretpostavku nedužnosti te pravo na dobru upravu. Povrh tih prava, važno je naglasiti činjenicu da djeca imaju posebna prava sadržana u članku 24. Povelje i u Konvenciji Ujedinjenih naroda o pravima djeteta, detaljnije razrađena u Općoj napomeni br. 25 Odbora UN-a o pravima djece u pogledu digitalnog okružja, kojima se zahtijeva da se vodi računa o njihovoj ranjivosti te da se osiguraju zaštita i skrb potrebni za njihovu dobrobit. Pri procjeni težine štete koju pojedini UI sustav može prouzročiti, među ostalim i u pogledu zdravlja i sigurnosti osoba, trebalo bi uzeti u obzir i temeljno pravo na visoku razinu zaštite okoliša koje je utvrđeno u Povelji i provodi se u politikama Unije.

- (49) Kad je riječ o visokorizičnim UI sustavima koji su sigurnosne komponente proizvoda ili sustava odnosno koji su sami proizvodi ili sustavi obuhvaćeni područjem primjene Uredbe (EZ) br. 300/2008 Europskog parlamenta i Vijeća²⁴, Uredbe (EU) br. 167/2013 Europskog parlamenta i Vijeća²⁵, Uredbe (EU) br. 168/2013 Europskog parlamenta i Vijeća²⁶, Direktive 2014/90/EU Europskog parlamenta i Vijeća²⁷, Direktive (EU) 2016/797 Europskog parlamenta i Vijeća²⁸, Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća²⁹,

²⁴ Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.).

²⁵ Uredba (EU) br. 167/2013 Europskog parlamenta i Vijeća od 5. veljače 2013. o homologaciji i nadzoru tržišta traktora za poljoprivredu i šumarstvo (SL L 60, 2.3.2013., str. 1.).

²⁶ Uredba (EU) br. 168/2013 Europskog parlamenta i Vijeća od 15. siječnja 2013. o homologaciji i nadzoru tržišta vozila na dva ili tri kotača i četverocikala (SL L 60, 2.3.2013., str. 52.).

²⁷ Direktiva 2014/90/EU Europskog parlamenta i Vijeća od 23. srpnja 2014. o pomorskoj opremi i stavljanju izvan snage Direktive Vijeća 96/98/EZ (SL L 257, 28.8.2014., str. 146.).

²⁸ Direktiva (EU) 2016/797 Europskog parlamenta i Vijeća od 11. svibnja 2016. o interoperabilnosti željezničkog sustava u Europskoj uniji (SL L 138, 26.5.2016., str. 44.).

²⁹ Uredba (EU) 2018/858 Europskog parlamenta i Vijeća od 30. svibnja 2018. o homologaciji i nadzoru tržišta motornih vozila i njihovih prikolica te sustava, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila, o izmjeni uredaba (EZ) br. 715/2007 i (EZ) br. 595/2009 te o stavljanju izvan snage Direktive 2007/46/EZ (SL L 151, 14.6.2018., str. 1.).

Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća³⁰ i Uredbe (EU) 2019/2144 Europskog parlamenta i Vijeća³¹, primjereno je te akte izmijeniti kako bi se osiguralo da Komisija, na temelju tehničkih i regulatornih posebnosti svakog sektora te bez uplitanja u postojeće mehanizme upravljanja, ocjenjivanja sukladnosti i izvršavanja te rad tijela koja su u njima utvrđena, pri donošenju svih relevantnih delegiranih akata ili provedbenih akata na temelju tih akata uzima u obzir obvezne zahtjeve za visokorizične UI sustave utvrđene u ovoj Uredbi.

³⁰ Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.).

³¹ Uredba (EU) 2019/2144 Europskog parlamenta i Vijeća od 27. studenoga 2019. o zahtjevima za homologaciju tipa za motorna vozila i njihove prikolice te za sustave, sastavne dijelove i zasebne tehničke jedinice namijenjene za takva vozila, u pogledu njihove opće sigurnosti te zaštite osoba u vozilima i nezaštićenih sudionika u cestovnom prometu, o izmjeni Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća i stavljanju izvan snage uredbi (EZ) br. 78/2009, (EZ) br. 79/2009 i (EZ) br. 661/2009 Europskog parlamenta i Vijeća i uredbi Komisije (EZ) br. 631/2009, (EU) br. 406/2010, (EU) br. 672/2010, (EU) br. 1003/2010, (EU) br. 1005/2010, (EU) br. 1008/2010, (EU) br. 1009/2010, (EU) br. 19/2011, (EU) br. 109/2011, (EU) br. 458/2011, (EU) br. 65/2012, (EU) br. 130/2012, (EU) br. 347/2012, (EU) br. 351/2012, (EU) br. 1230/2012 i (EU) 2015/166 (SL L 325, 16.12.2019., str. 1.).

- (50) Kad je riječ o UI sustavima koji su sigurnosne komponente proizvoda ili koji su sami proizvodi, a obuhvaćeni su područjem primjene određenog zakonodavstva Unije o usklađivanju navedenog u prilogu ovoj Uredbi, primjereno ih je klasificirati kao visokorizične na temelju ove Uredbe ako je dotični proizvod predmet postupka ocjenjivanja sukladnosti koji provodi tijelo za ocjenjivanje sukladnosti kao treća strana na temelju relevantnog zakonodavstva Unije o usklađivanju. Takvi su proizvodi osobito strojevi, igračke, dizala, oprema i zaštitni sustavi namijenjeni za korištenje u potencijalno eksplozivnim atmosferama, radijska oprema, tlačna oprema, oprema za rekreacijska plovila, žičare, aparati na plinovita goriva, medicinski proizvodi i *in vitro* dijagnostički medicinski proizvodi, automobili i zrakoplovi.
- (51) Klasifikacija UI sustava kao visokorizičnog na temelju ove Uredbe ne bi nužno trebala značiti da se proizvod čija je sigurnosna komponenta UI sustav ili da se sâm UI sustav kao proizvod smatra „visokorizičnim” na temelju kriterija utvrđenih u relevantnom zakonodavstvu Unije o usklađivanju koje se primjenjuje na taj proizvod. To se osobito odnosi na uredbe (EU) 2017/745 i (EU) 2017/746 ako je predviđeno da treća strana provodi ocjenjivanje sukladnosti za srednjorizične i visokorizične proizvode.

- (52) Kad je riječ o samostalnim UI sustavima, odnosno visokorizičnim UI sustavima koji nisu sigurnosne komponente proizvoda ili koji su sâmi proizvodi, primjereno ih je klasificirati kao visokorizične ako, s obzirom na njihovu namjenu, kod njih postoji visok rizik od štete za zdravlje i sigurnost ili temeljna prava osoba, uzimajući u obzir i težinu moguće štete i njezinu vjerojatnost nastanka, te ako se upotrebljavaju u nekoliko posebnih unaprijed definiranih područja navedenih u ovoj Uredbi. Utvrđivanje tih sustava temelji se na istoj metodologiji i kriterijima predviđenima i za sve buduće izmjene popisa visokorizičnih UI sustava koje bi Komisija trebala biti ovlaštena donijeti delegiranim aktima kako bi se uzeo u obzir brz tempo tehnološkog razvoja i moguće promjene u korištenju UI sustavâ.

- (53) Važno je pojasniti i da mogu postojati posebni slučajevi u kojima UI sustavi na koje se upućuje u unaprijed definiranim područjima navedenima u ovoj Uredbi ne dovode do znatnog rizika od štete za pravne interese zaštićene na temelju tih područja jer bitno ne utječu na donošenje odluka ili ne štete znatno tim interesima. Za potrebe ove Uredbe UI sustav koji bitno ne utječe na ishod donošenja odluka trebalo bi razumjeti kao UI sustav koji ne utječe na sadržaj, a time ni na ishod donošenja odluka, bilo da je odluke donose ljudi ili da je donošenje odluka automatizirano. UI sustav koji bitno ne utječe na ishod donošenja odluka mogao bi uključivati situacije u kojima je ispunjen jedan od sljedećih uvjeta ili više njih. Prvi takav uvjet trebao bi biti da je UI sustav namijenjen obavljanju uske postupovne zadaće, kao što je UI sustav koji pretvara nestrukturirane podatke u strukturirane podatke, UI sustav koji dolazne dokumente klasificira u kategorije ili UI sustav koji se upotrebljava za otkrivanje duplikata među velikim brojem primjena. Te su zadaće toliko uske i ograničene da predstavljaju samo ograničene rizike koji se ne povećavaju korištenjem UI sustava u kontekstu koji je naveden kao visokorizična upotreba u prilogu ovoj Uredbi. Drugi uvjet trebao bi biti da je zadaća koju obavlja UI sustav namijenjena poboljšanju rezultata prethodno završene ljudske aktivnosti koja može biti relevantna za potrebe visokorizičnih upotreba navedenih u prilogu ovog Uredbi. S obzirom na te značajke UI sustav samo je dodatak ljudskoj aktivnosti uz posljedično smanjeni rizik. Na primjer, taj bi se uvjet primjenjivao na UI sustave namijenjene poboljšanju jezika koji se upotrebljava u prethodno izrađenim dokumentima, primjerice u vezi s profesionalnim tonom, akademskim stilom jezika ili usklađivanjem teksta s određenim porukama robne marke.

Treći uvjet trebao bi biti da je namjena UI sustava otkrivanje obrazaca donošenja odluka ili odstupanja od prethodnih obrazaca donošenja odluka. Rizik bi se smanjio jer korištenje UI sustava slijedi nakon prethodno dovršene ljudske procjene, koju ono ne namjerava zamijeniti niti utjecati na nju bez odgovarajućeg preispitivanja koje provodi čovjek. Takvi UI sustavi obuhvaćaju, na primjer, sustave koji se na temelju određenog obrasca nastavnikova ocjenjivanja mogu upotrebljavati za *ex post* provjeru toga je li nastavnik možda odstupio od svojeg obrasca ocjenjivanja kako bi se upozorilo na moguće nedosljednosti ili nepravilnosti. Četvrti uvjet trebao bi biti da je UI sustav namijenjen obavljanju zadaće koja je samo pripremna za procjenu relevantnu za svrhe UI sustava navedenih u prilogu ovoj Uredbi, čime se mogući učinak izlaznih vrijednosti sustava čini vrlo niskim u smislu predstavljanja rizika za procjenu koja treba uslijediti. Taj uvjet obuhvaća, među ostalim, pametna rješenja za postupanje s datotekama, koja uključuju različite funkcije poput indeksiranja, pretraživanja, obrade teksta i govora ili povezivanja podataka s drugim izvorima podataka, ili UI sustave koji se upotrebljavaju za prevođenje početnih dokumenata. U svakom slučaju, za UI sustave koji se upotrebljavaju u slučajevima visokih rizika koji su navedeni u prilogu ovoj Uredbi trebalo bi smatrati da predstavljaju znatne rizike od štete za zdravlje, sigurnost ili temeljna prava fizičkih osoba ako UI sustav podrazumijeva izradu profila u smislu članka 4. točke 4. Uredbe (EU) 2016/679 ili članka 3. točke 4. Direktive (EU) 2016/680 ili članka 3. točke 5. Uredbe (EU) 2018/1725. Kako bi se osigurala sljedivost i transparentnost, dobavljač koji na temelju prethodno navedenih uvjeta smatra da UI sustav nije visokorizičan trebao bi sastaviti dokumentaciju o ocjenjivanju prije nego što taj sustav bude stavljen na tržište ili u upotrebu i trebao bi tu dokumentaciju na zahtjev dostaviti nacionalnim nadležnim tijelima. Taj dobavljač trebao bi biti obvezan registrirati UI sustav u bazi podataka EU-a uspostavljenoj na temelju ove Uredbe. Kako bi se pružilo dodatno usmjeravanje za praktičnu provedbu uvjeta na temelju kojih UI sustavi navedeni u prilogu ovoj Uredbi iznimno nisu visokorizični, Komisija bi nakon savjetovanja s Vijećem za umjetnu inteligenciju trebala pružiti smjernice u kojima se precizira ta praktična provedba, dopunjene sveobuhvatnim popisom praktičnih primjera slučajeva upotrebe UI sustava koji su visokorizični i primjera upotrebe UI sustava koji nisu visokorizični.

- (54) Budući da biometrijski podaci čine posebnu kategoriju osobnih podataka, nekoliko kritičnih slučajeva korištenja biometrijskih sustava primjereno je klasificirati visokorizičnima, u mjeri u kojoj je njihovo korištenje dopušteno na temelju relevantnog prava Unije i nacionalnog prava. Tehničke netočnosti UI sustava namijenjenih daljinskoj biometrijskoj identifikaciji fizičkih osoba mogu rezultirati pristranim rezultatima i imati diskriminacijske učinke. Rizik od takvih pristranih rezultata i diskriminacijskih učinaka osobito je relevantna s obzirom na dob, etničku pripadnost, rasu, spol ili invaliditet. Stoga bi sustave za daljinsku biometrijsku identifikaciju trebalo klasificirati kao visokorizične s obzirom na rizike koje predstavljaju. Takva klasifikacija isključuje UI sustave namijenjene za biometrijsku provjeru, uključujući autentifikaciju, čija je jedina svrha potvrditi da je određena fizička osoba doista osoba kojom se predstavlja i potvrditi identitet fizičke osobe isključivo u svrhu pristupa usluzi, otključavanja uređaja ili sigurnog pristupa prostorijama. Osim toga, UI sustave namijenjene za biometrijsku kategorizaciju u skladu s osjetljivim atributima ili značajkama zaštićenima na temelju članka 9. stavka 1. Uredbe (EU) 2016/679 na osnovi biometrijskih podataka, u mjeri u kojoj nisu zabranjeni na temelju ove Uredbe, i sustave za prepoznavanje emocija koji nisu zabranjeni na temelju ove Uredbe trebalo bi klasificirati kao visokorizične. Biometrijski sustavi namijenjeni isključivo za omogućavanje kibernetičke sigurnosti i mjera zaštite osobnih podataka ne bi se trebali smatrati visokorizičnim UI sustavima.

- (55) Kad je riječ o upravljanju kritičnom infrastrukturom i njezinu radu, primjereno je kao visokorizične klasificirati one UI sustave koji su namijenjeni upotrebi kao sigurnosne komponente u upravljanju kritičnom digitalnom infrastrukturom navedenom u točki 8. Priloga Direktivi (EU) 2022/2557 i radu takve infrastrukture, u cestovnom prometu te u opskrbi vodom, plinom, grijanjem i električnom energijom jer bi njihov kvar ili neispravnost mogli ugroziti život i zdravlje osoba u velikim razmjerima te znatno poremetiti uobičajeno odvijanje društvenih i gospodarskih aktivnosti. Sigurnosne komponente kritične infrastrukture, uključujući kritičnu digitalnu infrastrukturu, sustavi su koji se upotrebljavaju za izravnu zaštitu fizičkog integriteta kritične infrastrukture ili zdravlja i sigurnosti osoba i imovine, ali koji nisu potrebni za funkcioniranje sustava. Kvar ili neispravnost takvih komponenti može izravno dovesti do rizika za fizički integritet kritične infrastrukture, a time i do rizika za zdravlje i sigurnost osoba i imovine. Komponente namijenjene korištenju isključivo u svrhe kibernetičke sigurnosti ne bi trebalo smatrati sigurnosnim komponentama. Primjeri sigurnosnih komponenti takve kritične infrastrukture mogu uključivati sustave za praćenje tlaka vode ili sustave za kontrolu protupožarnog alarma u centrima za računalstvo u oblaku.

- (56) Uvođenje UI sustavâ u obrazovanje važno je kako bi se promicalo visokokvalitetno digitalno obrazovanje i osposobljavanje te kako bi se svim učenicima i nastavnicima omogućilo da steknu i dijele potrebne digitalne vještine i kompetencije, uključujući medijsku pismenost i kritičko razmišljanje, kako bi aktivno sudjelovali u gospodarstvu, društvu i demokratskim procesima. Međutim, UI sustave koji se upotrebljavaju u obrazovanju ili strukovnom osposobljavanju, osobito za odlučivanje o pristupu ili upisu, za razvrstavanje osoba u ustanove ili programe za obrazovanje i strukovno osposobljavanje na svim razinama, za evaluaciju ishoda učenja osoba, za procjenu odgovarajuće razine obrazovanja pojedinca i bitan utjecaj na razinu obrazovanja i osposobljavanja koju će pojedinci steći ili kojoj će moći pristupiti odnosno za praćenje i otkrivanje zabranjenog ponašanja učenika tijekom testiranja trebalo bi klasificirati kao visokorizične UI sustavi jer mogu odrediti obrazovni i profesionalni tijek života osobe i stoga mogu utjecati na njezinu mogućnost da osigura sredstva za život. Ako se dizajniraju i upotrebljavaju na nepravilan način, takvi sustavi mogu biti osobito intruzivni i kršiti pravo na obrazovanje i osposobljavanje i pravo na nediskriminaciju te perpetuirati povijesne obrasce diskriminacije, primjerice protiv žena, određenih dobnih skupina, osoba s invaliditetom odnosno osoba određenog rasnog ili etničkog podrijetla ili seksualne orijentacije.

- (57) UI sustavi koji se upotrebljavaju za zapošljavanje, kadrovsko upravljanje i pristup samozapošljavanju, osobito za zapošljavanje i odabir osoba, za donošenje odluka koje utječu na uvjete radnog odnosa, promaknuće ili otkazivanje radnih ugovornih odnosa, za dodjelu zadataka na osnovi individualnog ponašanja, osobnih obilježja ili značajki i za praćenje ili evaluaciju osoba u radnim ugovornim odnosima također bi trebali biti klasificirani kao visokorizični jer bi ti sustavi mogli znatno utjecati na buduće izgleda za razvoj karijere, sredstva za život tih osoba i radnička prava. Relevantni radni ugovorni odnosi trebali bi na smislen način uključivati zaposlenike i osobe koji pružaju usluge putem platformi kako je navedeno u programu rada Komisije za 2021. U cijelom procesu zapošljavanja i pri evaluaciji, promaknuću ili zadržavanju osoba u radnim ugovornim odnosima takvi sustavi mogu perpetuirati povijesne obrasce diskriminacije, primjerice protiv žena, određenih dobni skupina, osoba s invaliditetom odnosno osoba određenog rasnog ili etničkog podrijetla ili seksualne orijentacije. UI sustavi koji se upotrebljavaju za praćenje učinkovitosti i ponašanja takvih osoba mogu ujedno narušavati njihova temeljna prava na zaštitu osobnih podataka i privatnost.

- (58) Još jedno područje u kojem UI sustavima treba posvetiti posebnu pozornost jest dostupnost i uživanje određenih osnovnih privatnih i javnih usluga i naknada potrebnih za potpuno sudjelovanje u društvu ili poboljšanje životnog standarda osoba. Osobito, fizičke osobe koje podnose zahtjev za osnovne naknade i usluge javne pomoći od tijela javne vlasti ili ih od njih primaju, odnosno zdravstvene usluge, naknade socijalne sigurnosti, socijalne usluge kojima se pruža zaštita u slučajevima kao što su majčinstvo, bolest, nesreće na radu, uzdržavanost ili starost i gubitak zaposlenja te socijalna i stambena pomoć, obično ovise o tim naknadama i uslugama te su u ranjivom položaju u odnosu na nadležna tijela. Ako se UI sustavi upotrebljavaju za određivanje toga trebaju li tijela takve naknade i usluge dodijeliti, uskratiti, smanjiti, ukinuti ili tražiti njihov povrat, uključujući određivanje toga imaju li korisnici legitimno pravo na takve naknade ili usluge, ti sustavi mogu znatno utjecati na sredstva za život tih osoba i kršiti njihova temeljna prava, kao što je pravo na socijalnu zaštitu, nediskriminaciju, ljudsko dostojanstvo ili djelotvorno pravno sredstvo, te bi ih stoga trebalo klasificirati kao visokorizične. Međutim, ova Uredba ne bi trebala otežavati razvoj i primjenu inovativnih pristupa u javnoj upravi, koja bi imala koristi od šire upotrebe usklađenih i sigurnih UI sustava, pod uvjetom da ti sustavi ne podrazumijevaju velik rizik za pravne i fizičke osobe.

Usto, UI sustave koji se upotrebljavaju za evaluaciju kreditnog rejtinga ili kreditne sposobnosti fizičkih osoba trebalo bi klasificirati kao visokorizične jer određuju pristup tih osoba financijskim resursima ili osnovnim uslugama kao što su stanovanje, električna energija i telekomunikacijske usluge. UI sustavi koji se upotrebljavaju u tu svrhu mogu dovesti do diskriminacije osoba ili skupina te perpetuirati povijesne obrasce diskriminacije, primjerice na temelju rasnog ili etničkog podrijetla, roda, invaliditeta, dobi ili seksualne orijentacije, ili mogu stvoriti nove vrste diskriminacijskih učinaka. Međutim, UI sustavi predviđeni pravom Unije u svrhu otkrivanja prijevara u ponudi financijskih usluga i u bonitetne svrhe za izračun kapitalnih zahtjeva kreditnih institucija i društava za osiguranje ne bi se trebali smatrati visokorizičnima na temelju ove Uredbe. Nadalje, UI sustavi namijenjeni procjeni rizika i određivanju cijena u odnosu na fizičke osobe za zdravstveno i životno osiguranje mogu znatno utjecati i na sredstva za život tih osoba, a ako nisu propisno dizajnirani, razvijeni i korišteni, mogu kršiti njihova temeljna prava i dovesti do ozbiljnih posljedica za život i zdravlje ljudi, uključujući financijsku isključenost i diskriminaciju. Na kraju, UI sustavi koji se upotrebljavaju za evaluaciju i klasifikaciju hitnih poziva fizičkih osoba ili za dispečiranje ili određivanje prioriteta pri dispečiranju hitnih službi, uključujući policiju, vatrogasce i medicinsku pomoć, kao i sustavi za trijažu pacijenata pri pružanju hitne skrbi, isto bi se trebali smatrati visokorizičnima jer donose odluke u situacijama koje su kritične za život i zdravlje osoba te za njihovu imovinu.

- (59) S obzirom na njihovu ulogu i odgovornost, postupcima tijelâ kaznenog progona koji uključuju određene oblike korištenja UI sustavâ svojstvena je znatna neravnoteža moći i mogu dovesti do nadzora, uhićenja ili oduzimanja slobode fizičkih osoba, kao i do drugih nepovoljnih učinaka na temeljna prava zajamčena Poveljom. Posebice, ako UI sustav nije treniran s pomoću visokokvalitetnih podataka, ne ispunjava odgovarajuće zahtjeve u pogledu svoje učinkovitosti, točnosti ili otpornosti ili nije pravilno dizajniran i testiran prije stavljanja na tržište ili u upotrebu, može izdvajati ljude na diskriminatoran ili na drugačije netočan ili nepravedan način. Nadalje, ostvarivanje važnih postupovnih temeljnih prava, kao što su pravo na djelotvorno pravno sredstvo i na pošteno suđenje te pravo na obranu i pretpostavku nedužnosti, moglo bi biti otežano, osobito ako takvi UI sustavi nisu dovoljno transparentni, objašnjivi i dokumentirani. Stoga je primjereno, u mjeri u kojoj je njihovo korištenje dopušteno na temelju relevantnog prava Unije i nacionalnog prava, klasificirati kao visokorizične one UI sustave koji su namijenjeni korištenju u kontekstu kaznenog progona ako su točnost, pouzdanost i transparentnost osobito važne kako bi se izbjegli nepovoljni utjecaji, zadržalo povjerenje javnosti te osigurala odgovornost i djelotvorna pravna zaštita.

S obzirom na prirodu tih aktivnosti i s njima povezane rizike, ti visokorizični UI sustavi trebali bi osobito uključivati UI sustave namijenjene za korištenje od strane tijela kaznenog progona ili u njihovo ime ili za korištenje od strane institucija, tijela, ureda ili agencija Unije radi potpore tijelima kaznenog progona za procjenu rizika fizičke osobe da postane žrtva kaznenih djela, kao poligrafi i slični alati, za evaluaciju pouzdanosti dokaza tijekom istrage ili progona kaznenih djela i, u mjeri u kojoj to nije zabranjeno na temelju ove Uredbe, za procjenu rizika da fizička osoba počini ili ponovno počini kazneno djelo ne isključivo na osnovi izrade profila fizičkih osoba ili procjene osobina i značajki ili prethodnog kriminalnog ponašanja fizičkih osoba ili skupina, za izradu profila tijekom otkrivanja, istrage ili progona kaznenih djela. UI sustave posebno namijenjene za upravne postupke poreznih i carinskih tijela i financijsko-obavještajnih jedinica koje provode administrativne zadaće analize informacija na temelju prava Unije o sprečavanju pranja novca ne bi trebalo klasificirati kao visokorizične UI sustave koje tijela kaznenog progona upotrebljavaju u svrhu sprečavanja, otkrivanja, istrage i progona kaznenih djela. Tijela kaznenog progona ni druga relevantna tijela ne bi smjela koristiti UI alate tako da postanu čimbenik nejednakosti ili isključenosti. Ne bi se trebao zanemariti utjecaj korištenja UI alata na prava osumnjičenika na obranu, osobito s obzirom na poteškoću u dobivanju smislenih informacija o funkcioniranju tih sustava i posljedičnu poteškoću u osporavanju njihovih rezultata na sudu, osobito za fizičke osobe pod istragom.

- (60) UI sustavi koji se upotrebljavaju u području migracija, azila i upravljanja nadzorom državne granice utječu na osobe koje su često u osobito ranjivu položaju i koje ovise o ishodu postupaka nadležnih tijela javne vlasti. Točnost, nediskriminacija i transparentnost UI sustava koji se upotrebljavaju u tim kontekstima stoga su posebno važne kako bi se zajamčilo poštovanje temeljnih prava zahvaćenih osoba, osobito njihovih prava na slobodno kretanje, nediskriminaciju, zaštitu privatnog života i osobnih podataka, međunarodnu zaštitu i dobru upravu. Stoga je primjereno klasificirati kao visokorizične, u mjeri u kojoj je njihovo korištenje dopušteno na temelju relevantnog prava Unije i nacionalnog prava, UI sustave namijenjene za korištenje od strane nadležnih tijela javne vlasti ili institucija, tijela, ureda ili agencija Unije ili u njihovo ime, a koji su zaduženi za zadaće u području migracija, azila i upravljanja nadzorom državne granice, kao poligrafe i slične alate, za procjenu određenih rizika koje predstavljaju fizičke osobe koje ulaze na državno područje države članice ili podnose zahtjev za vizu ili azil, za pomoć nadležnim tijelima javne vlasti u razmatranju, uključujući povezanu procjenu pouzdanosti dokaza, zahtjevâ za azil, viza i boravišnih dozvola te povezanih pritužbi u pogledu cilja utvrđivanja prihvatljivosti fizičkih osoba koje podnose zahtjev za određeni status, u svrhu otkrivanja, priznavanja ili identifikacije fizičkih osoba u kontekstu migracija, azila i upravljanja nadzorom državne granice, uz iznimku provjere putnih isprava.

UI sustavi koji se upotrebljavaju u području migracija, azila i upravljanja nadzorom državne granice obuhvaćeni ovom Uredbom trebali bi biti u skladu s relevantnim postupovnim zahtjevima utvrđenima Uredbom (EZ) 810/2009 Europskog parlamenta i Vijeća³², Direktivom 2013/32/EU Europskog parlamenta i Vijeća³³ i drugim relevantnim pravom Unije. Države članice odnosno institucije, tijela, uredi ili agencije Unije ni u kojem slučaju ne bi smjeli koristiti UI sustave u području migracija, azila i upravljanja nadzorom državne granice kao sredstvo za zaobilaženje svojih međunarodnih obveza na temelju Konvencije UN-a o statusu izbjeglica potpisane u Ženevi 28. srpnja 1951., kako je izmijenjena Protokolom od 31. siječnja 1967. Njima se ne bi trebalo ni na koji način kršiti načelo zabrane prisilnog udaljenja ili vraćanja niti uskraćivati sigurne i djelotvorne zakonite načine za dolazak na područje Unije, uključujući pravo na međunarodnu zaštitu.

³² Uredba (EZ) br. 810/2009 Europskog parlamenta i Vijeća od 13. srpnja 2009. o uspostavi Zakonika Zajednice o vizama (Zakonik o vizama) (SL L 243, 15.9.2009., str. 1.).

³³ Direktiva 2013/32/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o zajedničkim postupcima za priznavanje i oduzimanje međunarodne zaštite (SL L 180, 29.6.2013., str. 60.).

- (61) Određene UI sustave namijenjene sudovanju i demokratskim procesima trebalo bi klasificirati kao visokorizične s obzirom na njihov potencijalno velik utjecaj na demokraciju, vladavinu prava, osobne slobode te pravo na djelotvoran pravno sredstvo i na pošteno suđenje. Točnije, radi odgovora na rizike od mogućih pristranosti, pogrešaka i netransparentnosti, primjereno je klasificirati kao visokorizične one UI sustave koji su namijenjeni korištenju od strane pravosudnog tijela ili u njegovo ime za pomoć pravosudnim tijelima u istraživanju i tumačenju činjenica i prava te primjeni prava na konkretan skup činjenica. UI sustavi namijenjeni korištenju od strane tijela za alternativno rješavanje sporova u te svrhe također bi se trebali smatrati visokorizičnima ako ishodi postupka alternativnog rješavanja sporova proizvode pravne učinke za stranke. Alati umjetne inteligencije mogu biti potpora ovlasti sudaca za donošenje odluka ili neovisnosti sudstva, ali ih ne bi smjeli zamijeniti: konačno donošenje odluka mora i dalje biti aktivnost koju obavljaju ljudi. Klasifikacija UI sustava kao visokorizičnih ne bi se trebala odnositi na UI sustave namijenjene isključivo pomoćnim administrativnim aktivnostima koje ne utječu na stvarno sudovanje u pojedinačnim slučajevima, kao što su anonimizacija ili pseudonimizacija sudskih odluka, dokumenata ili podataka, komunikacija među osobljem ili administrativne zadaće.

- (62) Ne dovodeći u pitanja pravila predviđena u Uredbi (EU) 2024/... Europskog parlamenta i Vijeća³⁴⁺, te kako bi se uklonili rizici od neopravdanog vanjskog uplitanja u pravo glasa utvrđeno u članku 39. Povelje i od nerazmjernih učinaka na demokraciju i vladavinu prava, UI sustave namijenjene za korištenje kako bi se utjecalo na ishod izbora ili referendumu ili na ponašanje fizičkih osoba tijekom glasovanja na izborima ili referendumima trebalo bi klasificirati kao visokorizične UI sustave, uz iznimku UI sustava čijim izlaznim vrijednostima fizičke osobe nisu izravno izložene, kao što su alati koji se upotrebljavaju za organizaciju, optimizaciju i strukturiranje političkih kampanja s administrativnog i logističkog stajališta.
- (63) Činjenicu da je pojedini UI sustav klasificiran kao visokorizičan na temelju ove Uredbe ne bi trebalo tumačiti kao da je korištenje tog sustava zakonito na temelju drugih pravnih akata Unije ili nacionalnog prava usklađenog s pravom Unije, primjerice prava o zaštiti osobnih podataka, o korištenju poligrafa i sličnih alata ili drugih sustava kojima se utvrđuje emocionalno stanje fizičkih osoba. Svako takvo korištenje trebalo bi se i dalje ostvarivati samo u skladu s primjenjivim zahtjevima koji proizlaze iz Povelje te primjenjivih akata sekundarnog prava Unije i nacionalnog prava. Ovu Uredbu ne bi trebalo tumačiti kao pružanje pravne osnove za obradu osobnih podataka, uključujući, ako je to relevantno, posebne kategorije osobnih podataka, osim ako je u ovoj Uredbi izričito predviđeno drugačije.

³⁴ Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o transparentnosti i ciljanju u političkom oglašavanju (SL L,..., ELI: ...).

⁺ SL: molimo u tekst umetnuti broj Uredbe iz PE 90/23 (2021/0381(COD)) i dopuniti odgovarajuću bilješku.

- (64) Kako bi se smanjili rizici visokorizičnih UI sustava koji su stavljeni na tržište ili u upotrebu i kako bi se osigurala visoka razina pouzdanosti, na visokorizične UI sustave trebali bi se primjenjivati određeni obvezni zahtjevi, uzimajući u obzir namjenu i kontekst korištenja UI sustava i u skladu sa sustavom upravljanja rizikom koji treba uspostaviti dobavljač. Mjerama koje dobavljači donose radi usklađivanja s obveznim zahtjevima ove Uredbe trebalo bi uzeti u obzir općepriznata najnovija dostignuća u području umjetne inteligencije i te bi mjere trebale biti razmjerne i djelotvorne za postizanje ciljeva ove Uredbe. Na temelju novog zakonodavnog okvira, kako je pojašnjeno u obavijesti Komisije pod nazivom „Plavi vodič’ o provedbi pravila EU-a o proizvodima 2022.”, opće je pravilo da se više od jednog pravnog akta zakonodavstva Unije o usklađivanju može primjenjivati na jedan proizvod jer se stavljanje na raspolaganje ili u upotrebu može provesti samo ako je proizvod u skladu sa svim primjenjivim zakonodavstvom Unije o usklađivanju. Opasnosti UI sustavâ obuhvaćene zahtjevima ove Uredbe odnose se na različite aspekte od onih u postojećem zakonodavstvu Unije o usklađivanju te bi se stoga zahtjevima ove Uredbe dopunio postojeći skup zakonodavstva Unije o usklađivanju. Na primjer, strojevi ili medicinski proizvodi u koje je ugrađen UI sustav mogli bi predstavljati rizike koji nisu obuhvaćeni osnovnim zdravstvenim i sigurnosnim zahtjevima utvrđenima u relevantnom zakonodavstvu Unije o usklađivanju jer se to sektorsko pravo ne bavi rizicima specifičnima za UI sustave.

Zbog toga je potrebna istovremena i komplementarna primjena raznih zakonodavnih akata. Kako bi se osigurala dosljednost i izbjeglo nepotrebno administrativno opterećenje i nepotrebni troškovi, dobavljači proizvoda koji sadržava jedan ili više visokorizičnih UI sustava, na koje se primjenjuju zahtjevi iz ove Uredbe i zahtjevi iz zakonodavstva Unije o usklađivanju na temelju novog zakonodavnog okvira i navedeni u prilogu ovoj Uredbi, trebali bi biti fleksibilni u pogledu operativnih odluka o tome kako na najbolji način osigurati usklađenost proizvoda koji sadržava jedan ili više UI sustava sa svim primjenjivim zahtjevima zakonodavstva Unije o usklađivanju. Ta bi fleksibilnost mogla značiti, na primjer, odluku dobavljača da dio potrebnih postupaka testiranja i izvješćivanja, informacija i dokumentacije koji se zahtijevaju na temelju ove Uredbe integrira u već postojeću dokumentaciju i postupke koji se zahtijevaju na temelju postojećeg zakonodavstva Unije o usklađivanju koje se temelji na novom zakonodavnom okviru i koje je navedeno u prilogu ovoj Uredbi. To ni na koji način ne bi trebalo umanjiti obvezu dobavljača da poštuje sve primjenjive zahtjeve.

- (65) Sustav upravljanja rizikom trebao bi se sastojati od kontinuiranog iterativnog procesa koji se planira i izvodi tijekom cijelog životnog ciklusa visokorizičnog UI sustava. Taj bi proces trebao biti usmjeren na utvrđivanje i ublažavanje relevantnih rizika UI sustavâ za zdravlje, sigurnost i temeljna prava. Sustav upravljanja rizikom trebalo bi redovito preispitivati i ažurirati kako bi se osigurala njegova kontinuirana djelotvornost, kao i obrazlaganje i dokumentiranje svih važnih donesenih odluka i poduzetih mjera koje podliježu ovoj Uredbi. Tim bi procesom trebalo osigurati da dobavljač utvrdi rizike ili nepovoljne učinke i provede mjere za ublažavanje poznatih i razumno predvidljivih rizika UI sustavâ za zdravlje, sigurnost i temeljna prava s obzirom na njihovu namjenu i razumno predvidljivu pogrešnu upotrebu, uključujući moguće rizike koji proizlaze iz interakcije između UI sustava i okružja u kojem djeluje. Sustav upravljanja rizikom trebao bi primjenjivati najprikladnije mjere upravljanja rizikom s obzirom na najnovija dostignuća u području umjetne inteligencije. Pri utvrđivanju najprikladnijih mjera upravljanja rizikom dobavljač bi trebao dokumentirati i objasniti donesene odluke te, prema potrebi, uključiti stručnjake i vanjske dionike. Pri utvrđivanju razumno predvidljive pogrešne upotrebe visokorizičnih UI sustava dobavljač bi trebao obuhvatiti korištenja UI sustavâ za koja se, iako nisu izravno obuhvaćena namjenom i navedena u uputama za korištenje, ipak može razumno pretpostaviti da će proizaći iz lako predvidljivog ljudskog ponašanja u kontekstu specifičnih značajki i korištenja određenog UI sustava. Sve poznate i predvidljive okolnosti povezane s korištenjem visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive pogrešne upotrebe, koja može prouzročiti rizike za zdravlje i sigurnost ili temeljna prava, trebale bi biti navedene u uputama za korištenje koje pruža dobavljač. Time treba osigurati da ih je subjekt koji uvodi sustav svjestan i da ih uzme u obzir pri korištenju visokorizičnog UI sustava. Utvrđivanje i provedba mjera za ublažavanje rizika od predvidljive pogrešne upotrebe na temelju ove Uredbe ne bi trebali iziskivati posebno dodatno osposobljavanje za visokorizični UI sustav od strane dobavljača kako bi ih se riješila razumno predvidljiva pogrešna upotreba. Međutim, dobavljače se potiče da razmotre takve dodatne mjere osposobljavanja kako bi se ublažile razumno predvidljive pogrešne upotrebe ako je to potrebno i primjereno.

- (66) Zahtjevi bi se trebali primjenjivati na visokorizične UI sustave u pogledu upravljanja rizikom, kvalitete i relevantnosti korištenih skupova podataka, tehničke dokumentacije i vođenja evidencije, transparentnosti i pružanja informacija subjektima koji uvode sustav, ljudskog nadzora te otpornosti, točnosti i kibernetičke sigurnosti. Ti su zahtjevi potrebni kako bi se djelotvorno ublažili rizici za zdravlje, sigurnost i temeljna prava. S obzirom na to da druge mjere kojima se manje ograničava trgovina nisu u razumnoj mjeri dostupne ti zahtjevi nisu neopravdana ograničenja u području trgovine.

- (67) Visokokvalitetni podaci i pristup njima imaju ključnu ulogu u pružanju strukture i osiguravanju učinkovitosti mnogih UI sustava, posebno kad se upotrebljavaju tehnike s treniranjem modelâ, s ciljem da visokorizični UI sustav funkcionira kako je predviđeno i sigurno te da ne postane izvor diskriminacije koja je zabranjena pravom Unije.
- Visokokvalitetni skupovi podataka za treniranje, validaciju i testiranje zahtijevaju provedbu odgovarajućih praksi upravljanja i rukovanja podacima. Skupovi podataka za treniranje, validaciju i testiranje, uključujući oznake, trebali bi biti relevantni, dovoljno reprezentativni i u najvećoj mogućoj mjeri biti bez pogrešaka te potpuni s obzirom na namjenu sustava. Kako bi se olakšala usklađenost s pravom Unije o zaštiti podataka, kao što je Uredba (EU) 2016/679, prakse upravljanja i rukovanja podacima trebale bi u slučaju osobnih podataka uključivati transparentnost u vezi s izvornom svrhom prikupljanja podataka. Skupovi podataka trebali bi imati i odgovarajuća statistička obilježja, među ostalim i u pogledu osoba ili skupina osoba u vezi s kojima se visokorizični UI sustav namjerava koristiti, pri čemu se posebna pažnja posvećuje ublažavanju mogućih pristranosti u skupovima podataka, koje bi mogle utjecati na zdravlje i sigurnost osoba, negativno utjecati na temeljna prava ili dovesti do diskriminacije zabranjene pravom Unije, osobito ako izlazne vrijednosti utječu na ulazne vrijednosti za buduće operacije (povratne veze). Pristranosti mogu primjerice biti inherentne temeljnim skupovima podataka, osobito kad se upotrebljavaju povijesni podaci, ili se mogu generirati kad se sustavi implementiraju u stvarnom svijetu.

Na rezultate koje pružaju UI sustavi mogle bi utjecati takve inherentne pristranosti koje imaju tendenciju postupnog povećanja, čime se perpetuira i pojačava postojeća diskriminacija, posebno za osobe koje pripadaju određenim skupinama ranjivih osoba, uključujući rasne ili etničke skupine. Zahtjev da skupovi podataka u najvećoj mogućoj mjeri budu potpuni i bez pogrešaka ne bi trebao utjecati na primjenu tehnika za zaštitu privatnosti u kontekstu razvoja i testiranja UI sustavâ. U skupovima podataka osobito se u obzir uzimaju, u mjeri u kojoj to iziskuje njihova namjena, obilježja, značajke ili elementi specifični za zemljopisno, kontekstualno, bihevioralno ili funkcionalno okružno u kojem se UI sustav namjerava upotrebljavati. Zahtjevi povezani s upravljanjem podacima mogu se ispuniti angažiranjem trećih strana koje nude certificirane usluge usklađivanja, uključujući provjeru upravljanja podacima, cjelovitosti skupa podataka te prakse treniranja, validacije i testiranja podataka, u mjeri u kojoj je osigurana usklađenost sa zahtjevima u pogledu podataka iz ove Uredbe.

- (68) Kad je riječ o razvoju i procjeni visokorizičnih UI sustava, određeni akteri, kao što su dobavljači, prijavljena tijela i drugi relevantni subjekti, na primjer europski centri za digitalne inovacije, centri za testiranje i eksperimentiranje te istraživači, trebali bi imati pristup visokokvalitetnim skupovima podataka unutar područja aktivnosti tih aktera povezanih s ovom Uredbom. Zajednički europski podatkovni prostori koje je uspostavila Komisija te olakšavanje razmjene podataka među poduzećima i s državnim upravama u javnom interesu bit će ključni za osiguravanje pouzdanog, odgovornog i nediskriminirajućeg pristupa visokokvalitetnim podacima za treniranje, validaciju i testiranje UI sustavâ. Na primjer, u području zdravstva zajednički europski prostor za zdravstvene podatke olakšat će nediskriminirajući pristup zdravstvenim podacima i treniranje algoritama umjetne inteligencije s pomoću tih skupova podataka tako da se očuvaju privatnost, sigurnost, pravovremenost, transparentnost i pouzdanost uz odgovarajuće institucijsko upravljanje. Relevantna nadležna tijela, uključujući sektorska tijela, koja pružaju ili olakšavaju pristup podacima, mogu olakšati i pružanje visokokvalitetnih podataka za treniranje, validaciju i testiranje UI sustavâ.
- (69) Pravo na privatnost i zaštitu osobnih podataka mora biti zajamčeno tijekom cijelog životnog ciklusa UI sustava. U tom su pogledu načela smanjenja količine podataka te tehničke i integrirane zaštite podataka, kako su utvrđena u pravu Unije o zaštiti podataka, primjenjiva tijekom obrade osobnih podataka. Mjere koje dobavljači poduzimaju kako bi osigurali usklađenost s tim načelima mogu uključivati ne samo anonimizaciju i kriptiranje, nego i upotrebu tehnologije kojom se omogućuje dovođenje algoritama u podatke i treniranje UI sustavâ bez prijenosa između strana ili kopiranja samih neobrađenih ili strukturiranih podataka, ne dovodeći u pitanje zahtjeve u pogledu upravljanja podacima predviđene u ovoj Uredbi.

- (70) Kako bi se prava drugih osoba zaštitila od diskriminacije koja bi mogla proizaći iz pristranosti UI sustavâ, dobavljači bi iznimno trebali, u mjeri u kojoj je to nužno u svrhu otkrivanja i ispravljanja pristranosti u vezi s visokorizičnim UI sustavima, podložno odgovarajućim zaštitnim mjerama za temeljna prava i slobode fizičkih osoba i nakon primjene svih primjenjivih uvjeta utvrđenih na temelju ove Uredbe, dodatno uz uvjete utvrđene u uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivi (EU) 2016/680, moći obrađivati i posebne kategorije osobnih podataka kao pitanje od znatnog javnog interesa u smislu članka 9. stavka 2. točke (g) Uredbe (EU) 2016/679 i članka 10. stavka 2. točke (g) Uredbe (EU) 2018/1725.
- (71) Postojanje razumljivih informacija o načinu na koji su visokorizični UI sustavi razvijeni i načinu njihova rada tijekom cijelog njihova životnog ciklusa ključno je za omogućivanje sljedivosti tih sustava, provjeru usklađenosti sa zahtjevima ove Uredbe te praćenje njihova rada i praćenje nakon stavljanja na tržište. Za to je potrebno vođenje evidencije i dostupnost tehničke dokumentacije koja sadržava informacije potrebne za procjenu usklađenosti UI sustava s relevantnim zahtjevima i olakšavanje praćenja nakon stavljanja na tržište. Takve informacije trebale bi uključivati opće značajke, sposobnosti i ograničenja sustava, algoritme, podatke, postupke treniranja, testiranja i validacije koji su primijenjeni, kao i dokumentaciju o relevantnom sustavu upravljanja rizikom te bi trebale biti sastavljene u obliku koji je jasan i razumljiv. Tehnička dokumentacija trebala bi se ažurirati na odgovarajući način tijekom cijelog životnog ciklusa UI sustava. Nadalje, kod visokorizičnih UI sustava trebalo bi biti tehnički omogućeno automatsko bilježenje događaja putem vođenja evidencije tijekom cijelog životnog ciklusa sustava.

- (72) Kako bi se pristupilo rješavanju problema povezanih s netransparentnošću i složenošću određenih UI sustava i pomoglo subjektima koji uvode UI sustav da ispune svoje obveze na temelju ove Uredbe, za visokorizične UI sustave trebalo bi zahtijevati transparentnost prije njihova stavljanja na tržište ili u upotrebu. Visokorizični UI sustavi trebali bi biti dizajnirani tako da subjekti koji ih uvode mogu razumjeti kako UI sustav funkcionira, evaluirati njegovu funkcionalnost te razumjeti njegove prednosti i ograničenja. Visokorizični UI sustavi trebali bi biti popraćeni odgovarajućim informacijama u obliku uputa za korištenje. Takve informacije trebale bi uključivati značajke, sposobnosti i ograničenja rada UI sustava. Oni bi obuhvaćali informacije o mogućim poznatim i predvidljivim okolnostima povezanim s korištenjem visokorizičnog UI sustava, uključujući djelovanje subjekta koji uvodi sustav koje može utjecati na ponašanje i učinkovitost sustava, u okviru kojeg UI sustav može prouzročiti rizike za zdravlje, sigurnost i temeljna prava, o promjenama koje je dobavljač unaprijed odredio i ocijenio u pogledu sukladnosti te o relevantnim mjerama ljudskog nadzora, uključujući mjere kojima se subjektima koji uvode sustav olakšava tumačenje izlaznih vrijednosti UI sustava. Transparentnost, uključujući popratne upute za korištenje, trebala bi pomoći subjektima koji uvode sustav pri njegovu korištenju i poduprijeti njihovo informirano donošenje odluka. Subjekti koji uvode sustav trebali bi, među ostalim, biti u boljoj poziciji da pravilno odaberu sustav koji namjeravaju upotrebljavati s obzirom na obveze koje se na njih primjenjuju, biti informirani o namjeravanim i isključenim upotrebama te pravilno i primjereno upotrebljavati UI sustav. Kako bi se poboljšale čitljivost i pristupačnost informacija sadržanih u uputama za korištenje, trebalo bi, prema potrebi, u njih uključiti ilustrativne primjere, na primjer o ograničenjima te o namjeravanim i isključenim upotrebama UI sustava. Dobavljači bi trebali osigurati da sva dokumentacija, uključujući upute za korištenje, sadržava smislene, sveobuhvatne, pristupačne i razumljive informacije, uzimajući u obzir potrebe i predvidljivo znanje ciljanih subjekata koji uvode sustav. Upute za korištenje trebale bi biti dostupne na jeziku koji bez poteškoća razumiju ciljani subjekti koji uvode sustav, a određuje ga dotična država članica.

- (73) Visokorizične UI sustave trebalo bi dizajnirati i razvijati tako da fizičke osobe mogu nadzirati njihovo funkcioniranje, osigurati da se upotrebljavaju kako je predviđeno i da se njihovi učinci rješavaju tijekom životnog ciklusa sustava. U tom bi cilju dobavljač sustava prije njegova stavljanja na tržište ili u upotrebu trebao utvrditi odgovarajuće mjere ljudskog nadzora. Prema potrebi takvim bi mjerama osobito trebalo osigurati da su u sustav ugrađena operativna ograničenja koja sam sustav ne može promijeniti i da on reagira na ljudske operatore te da fizičke osobe zadužene za ljudski nadzor imaju potrebne kompetencije, osposobljavanje i ovlasti za obavljanje te zadaće. Također je neophodno, prema potrebi, osigurati da visokorizični UI sustavi uključuju mehanizme za usmjeravanje i informiranje fizičke osobe zadužene za ljudski nadzor kako bi donijela informirane odluke o tome treba li, kada i kako intervenirati da bi se izbjegle negativne posljedice ili rizici odnosno sustav zaustavio ako ne funkcionira kako je predviđeno. S obzirom na znatne posljedice za osobe ako u određenim sustavima za biometrijsku identifikaciju dođe do netočnih rezultata, primjereno je za te sustave predvidjeti zahtjev u pogledu pojačanog ljudskog nadzora tako da subjekt koji uvodi sustav ne može poduzeti nikakve radnje ili odluke na temelju identifikacije proizišle iz sustava ako identifikaciju nisu zasebno provjerile i potvrdile najmanje dvije fizičke osobe. Te osobe mogle bi biti iz jednog ili više subjekata i mogle bi uključivati osobu koja upravlja sustavom ili ga upotrebljava. Taj zahtjev ne bi trebao predstavljati nepotrebno opterećenje ili uzrokovati kašnjenja i moglo bi biti dovoljno da se zasebne provjere koje provode različite osobe automatski bilježe u evidenciji koju generira sustav. S obzirom na posebnosti područjâ kaznenog progona, migracija, nadzora državne granice i azila, taj se zahtjev ne bi trebao primjenjivati ako se u skladu s pravom Unije ili nacionalnim pravom smatra da je primjena tog zahtjeva nerazmjerna.

- (74) Visokorizični UI sustavi trebali bi imati ujednačen učinak tijekom cijelog životnog ciklusa te posjedovati odgovarajuću razinu točnosti, otpornosti i kibernetičke sigurnosti s obzirom na njihovu namjenu i u skladu s općepriznatim najnovijim dostignućima. Komisija i relevantne organizacije i dionici potiču se da uzmu u obzir ublažavanje rizika i negativnih učinaka UI sustava. Očekivana razina parametara učinkovitosti trebala bi se navesti u popratnim uputama za korištenje. Dobavljači se pozivaju da te informacije dostave subjektima koji uvide sustav na jasan i lako razumljiv način, bez nesporazuma ili obmanjujućih izjava. Pravom Unije o zakonskom mjeriteljstvu, uključujući direktive 2014/31/EU³⁵ i 2014/32/EU³⁶ Europskog parlamenta i Vijeća, nastoji se osigurati točnost mjerenja te doprinijeti transparentnosti i pravednosti poslovnih transakcija. U tom kontekstu, u suradnji s relevantnim dionicima i organizacijama, kao što su tijela za mjeriteljstvo i utvrđivanje referentnih vrijednosti, Komisija bi prema potrebi trebala poticati razvoj referentnih vrijednosti i metodologija mjerenja za UI sustave. Komisija bi pritom trebala uzeti u obzir međunarodne partnere koji rade na mjeriteljstvu i relevantnim mjernim pokazateljima povezanim s umjetnom inteligencijom te surađivati s njima.

³⁵ Direktiva 2014/31/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na stavljanje na raspolaganje neautomatskih vaga na tržište (SL L 96, 29.3.2014., str. 107.).

³⁶ Direktiva 2014/32/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na stavljanje na raspolaganje mjernih instrumenata na tržištu (SL L 096, 29.3.2014., str. 149.).

- (75) Tehnička otpornost ključan je zahtjev za visokorizične UI sustave. Trebali bi biti otporni na štetno ili na drugi način nepoželjno ponašanje koje bi moglo proizaći iz ograničenjâ unutar sustava ili okružja u kojem sustavi rade (npr. pogreške, kvarovi, nedosljednosti, neočekivane situacije). Stoga bi trebalo poduzeti tehničke i organizacijske mjere kako bi se osigurala otpornost visokorizičnih UI sustava, na primjer dizajniranjem i razvojem odgovarajućih tehničkih rješenja za sprečavanje ili što veće smanjenje štetnog ili na drugi način nepoželjnog ponašanja. Ta tehnička rješenja mogu obuhvaćati, na primjer, mehanizme koji omogućuju sustavu da sigurno prekine svoj rad (sigurnosni planovi) u slučaju određenih anomalija ili ako se rad odvija izvan određenih unaprijed utvrđenih granica. Nepostojanje zaštite od tih rizika moglo bi imati posljedice za sigurnost ili negativno utjecati na temeljna prava, primjerice zbog pogrešnih odluka ili krivih ili pristranih izlaznih vrijednosti koje generira UI sustav.
- (76) Kibernetička sigurnost ključna je za otpornost UI sustavâ na pokušaje zlonamjernih trećih strana da iskoriste slabe točke tih sustava kako bi im izmijenili način korištenja, ponašanje, učinkovitost ili ugrozili njihova sigurnosna svojstva. U kibernetičkim napadima na UI sustave moguće je iskoristiti resurse specifične za umjetnu inteligenciju, kao što su skupovi podataka za treniranje (npr. trovanje podataka) ili istrenirani modeli (npr. neprijateljski napadi ili utvrđivanje pripadnosti) ili iskoristiti slabe točke digitalnih resursa UI sustava odnosno osnovne IKT infrastrukture. Kako bi se osigurala razina kibernetičke sigurnosti primjerena rizicima, dobavljači visokorizičnih UI sustava trebali bi stoga poduzeti odgovarajuće mjere, kao što su sigurnosne kontrole, prema potrebi uzimajući u obzir i osnovnu IKT infrastrukturu.

- (77) Ne dovodeći u pitanje zahtjeve koji se odnose na otpornost i točnost utvrđene u ovoj Uredbi, visokorizični UI sustavi obuhvaćeni područjem primjene uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima u skladu s tom uredbom mogu dokazati sukladnost s kibernetičkosigurnosnim zahtjevima ove Uredbe ispunjavanjem osnovnih kibernetičkosigurnosnih zahtjeva iz te uredbe. Ako visokorizični UI sustavi ispunjavaju osnovne zahtjeve iz uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima trebalo bi ih smatrati usklađenima s kibernetičkosigurnosnim zahtjevima utvrđenima u ovoj Uredbi u mjeri u kojoj je ispunjavanje tih zahtjeva dokazano u EU izjavi o sukladnosti izdanoj na temelju te uredbe ili u dijelovima te izjave. U tom cilju, tijekom procjene kibernetičkosigurnosnih rizika povezanih s proizvodima s digitalnim elementima koji su klasificirani kao visokorizični UI sustav u skladu s ovom Uredbom, koja se provodi na temelju uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima, trebalo bi uzeti u obzir rizike za kibernetičku otpornost UI sustava kad se radi o pokušajima neovlaštenih trećih strana da promijene njegovo korištenje, ponašanje ili učinkovitost, uključujući ranjivosti specifične za umjetnu inteligenciju kao što su trovanje podacima ili neprijateljski napadi, kao i, kada je to relevantno, rizike za temeljna prava kako je propisano ovom Uredbom.

- (78) Postupak ocjenjivanja sukladnosti predviđen ovom Uredbom trebao bi se primjenjivati u odnosu na osnovne kibernetičkosigurnosne zahtjeve za proizvod s digitalnim elementima obuhvaćen uredbom Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima koji je klasificiran kao visokorizični UI sustav na temelju ove Uredbe. Međutim, to pravilo ne bi trebalo rezultirati smanjenjem potrebne razine jamstva za kritične proizvode s digitalnim elementima obuhvaćene uredbom Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima.
- Stoga, odstupajući od tog pravila, visokorizični UI sustavi koji su obuhvaćeni područjem primjene ove Uredbe i ujedno su klasificirani kao važni i kritični proizvodi s digitalnim elementima na temelju uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima te na koje se primjenjuje postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole utvrđen u prilogu ovoj Uredbi podliježu odredbama o ocjenjivanju sukladnosti iz uredbe Europskog parlamenta i Vijeća o horizontalnim kibernetičkosigurnosnim zahtjevima za proizvode s digitalnim elementima u mjeri u kojoj se to odnosi na osnovne kibernetičkosigurnosne zahtjeve iz te uredbe. U tom bi se slučaju na sve ostale aspekte obuhvaćene ovom Uredbom trebale primjenjivati odgovarajuće odredbe o ocjenjivanju sukladnosti na temelju unutarnje kontrole utvrđene u prilogu ovoj Uredbi. Na osnovi znanja i stručnosti ENISA-e u području kibernetičkosigurnosne politike i zadaća dodijeljenih ENISA-i na temelju Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća³⁷, Komisija bi trebala surađivati s ENISA-om u pitanjima povezanim s kibernetičkom sigurnošću UI sustavâ.

³⁷ Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

- (79) Primjereno je da određena fizička ili pravna osoba, koja je definirana kao dobavljač, preuzme odgovornost za stavljanje visokorizičnog UI sustava na tržište ili u upotrebu, bez obzira na to je li ta fizička ili pravna osoba ista osoba koja je dizajnirala ili razvila sustav.
- (80) Kao potpisnice Konvencije Ujedinjenih naroda o pravima osoba s invaliditetom, Unija i države članice imaju pravnu obvezu štititi osobe s invaliditetom od diskriminacije i promicati njihovu ravnopravnost, osigurati da osobe s invaliditetom imaju pristup informacijskim i komunikacijskim tehnologijama i sustavima na ravnopravnoj osnovi te zajamčiti poštovanje privatnosti osoba s invaliditetom. S obzirom na sve veću važnost i upotrebu UI sustavâ, primjenom univerzalnih načela dizajna na sve nove tehnologije i usluge trebao bi se osigurati potpun i ravnopravan pristup za sve osobe na koje bi tehnologije umjetne inteligencije mogle utjecati ili koje te tehnologije upotrebljavaju, uključujući osobe s invaliditetom, na način kojim se u cijelosti poštuju njihovo inherentno dostojanstvo i raznolikost. Stoga je ključno da dobavljači osiguraju potpunu usklađenost sa zahtjevima u pogledu pristupačnosti, uključujući Direktivu (EU) 2016/2102 Europskog parlamenta i Vijeća³⁸ i Direktivu (EU) 2019/882. Dobavljači bi trebali osigurati integriranu usklađenost s tim zahtjevima. Stoga bi potrebne mjere trebalo što je više moguće uključiti u dizajn visokorizičnog UI sustava.

³⁸ Direktiva (EU) 2016/2102 Europskog parlamenta i Vijeća od 26. listopada 2016. o pristupačnosti internetskih stranica i mobilnih aplikacija tijela javnog sektora (SL L 327, 2.12.2016., str. 1.).

- (81) Dobavljač bi trebao uspostaviti pouzdan sustav upravljanja kvalitetom, osigurati realizaciju postupka ocjenjivanja sukladnosti koji se zahtijeva, sastaviti relevantnu dokumentaciju i uspostaviti pouzdan sustav praćenja nakon stavljanja na tržište. Dobavljači visokorizičnih UI sustava koji podliježu obvezama u pogledu sustavâ upravljanja kvalitetom u skladu s relevantnim sektorskim pravom Unije trebali bi imati mogućnost uključiti elemente sustava upravljanja kvalitetom predviđenog u ovoj Uredbi u postojeći sustav upravljanja kvalitetom predviđen u tom drugom sektorskom pravu Unije. Komplementarnost ove Uredbe i postojećeg sektorskog prava Unije trebala bi se uzeti u obzir i u budućim aktivnostima normizacije ili smjernicama koje donosi Komisija. Tijela javne vlasti koja stavljaju visokorizične UI sustave u upotrebu za vlastite potrebe mogu donijeti i provoditi pravila za sustav upravljanja kvalitetom u okviru sustava upravljanja kvalitetom donesenog na nacionalnoj ili regionalnoj razini, prema potrebi, uzimajući u obzir posebnosti sektora te nadležnosti i organizaciju dotičnog tijela javne vlasti.

- (82) Kako bi se omogućilo izvršavanje ove Uredbe i osigurali jednaki uvjeti za operatere te uzimajući u obzir različite oblike stavljanja digitalnih proizvoda na raspolaganje, važno je osigurati da osoba s poslovnim nastanom u Uniji u svim okolnostima može nadležnim tijelima pružiti sve potrebne informacije o usklađenosti pojedinog UI sustava. Stoga bi dobavljači s poslovnim nastanom u trećim zemljama trebali pisanim ovlaštenjem imenovati ovlaštenog zastupnika s poslovnim nastanom u Uniji prije stavljanja svojih UI sustava na raspolaganje u Uniji. Taj ovlašteni zastupnik ima ključnu ulogu u osiguravanju usklađenosti visokorizičnih UI sustava koje ti dobavljači koji nemaju poslovni nastan u Uniji stavljaju na tržište ili u upotrebu u Uniji i služi kao njihova osoba za kontakt s poslovnim nastanom u Uniji.
- (83) S obzirom na prirodu i složenost lanca vrijednosti za UI sustave te u skladu s načelima novog zakonodavnog okvira, ključno je osigurati pravnu sigurnost i olakšati usklađenost s ovom Uredbom. Stoga je potrebno pojasniti ulogu i posebne obveze relevantnih operatera duž tog lanca vrijednosti, kao što su uvoznici i distributeri koji mogu doprinijeti razvoju UI sustava. U određenim situacijama ti bi operateri mogli istodobno djelovati u više uloga i stoga bi trebali kumulativno ispunjavati sve relevantne obveze povezane s tim ulogama. Na primjer, operater bi mogao istodobno djelovati kao distributer i uvoznik.

- (84) Kako bi se zajamčila pravna sigurnost, potrebno je pojasniti da bi se pod određenim posebnim uvjetima svaki dobavljač, uvoznik, subjekt koji uvodi sustav ili treća strana trebali smatrati dobavljačem visokorizičnog UI sustava i stoga preuzeti sve relevantne obveze. To bi bio slučaj ako ta strana stavi svoje ime ili žig na visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu, ne dovodeći u pitanje ugovorne aranžmane u kojima je utvrđena drukčija raspodjela obveza. To bi bio slučaj i ako ta strana bitno izmijeni visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu na način da on i dalje bude visokorizičan u skladu s ovom Uredbom, ili ako izmijeni namjenu UI sustava, uključujući UI sustav opće namjene, koji nije bio klasificiran kao visokorizičan i već je stavljen na tržište ili u upotrebu, na način da UI sustav postane visokorizičan u skladu s ovom Uredbom. Te bi se odredbe trebale primjenjivati ne dovodeći u pitanje detaljnije odredbe utvrđene u određenom zakonodavstvu Unije o usklađivanju na temelju novog zakonodavnog okvira, zajedno s kojima bi se ova Uredba trebala primjenjivati. Na primjer, članak 16. stavak 2. Uredbe (EU) 2017/745, u kojem se navodi da određene promjene ne bi trebalo smatrati izmjenama proizvoda koje mogu utjecati na njegovu usklađenost s primjenjivim zahtjevima, trebao bi se i dalje primjenjivati na visokorizične UI sustave koji su medicinski proizvodi u smislu te uredbe.

- (85) UI sustavi opće namjene mogu se upotrebljavati samostalno kao visokorizični UI sustavi ili mogu biti komponente drugih visokorizičnih UI sustava. Stoga, zbog njihove specifične prirode i radi jamčenja pravedne podjele odgovornosti diljem lanca vrijednosti umjetne inteligencije, neovisno o tome mogu li ih drugi dobavljači upotrebljavati samostalno kao visokorizične UI sustave ili kao komponente visokorizičnih UI sustava i ako na temelju ove Uredbe nije drugačije predviđeno, dobavljači takvih sustava trebali bi blisko surađivati s dobavljačima relevantnih visokorizičnih UI sustava kako bi im se omogućilo ispunjavanje relevantnih obveza na temelju ove Uredbe i s nadležnim tijelima osnovanima na temelju ove Uredbe.
- (86) Ako se u skladu s uvjetima utvrđenima u ovoj Uredbi dobavljač koji je prvotno stavio UI sustav na tržište ili u upotrebu više ne smatra dobavljačem za potrebe ove Uredbe i ako taj dobavljač nije izričito isključio pretvaranje UI sustava u visokorizični UI sustav, bivši dobavljač ipak bi trebao blisko surađivati i staviti na raspolaganje potrebne informacije te pružiti razumno očekivani tehnički pristup i drugu pomoć koji su potrebni za ispunjavanje obveza utvrđenih u ovoj Uredbi, posebno u pogledu usklađenosti s ocjenjivanjem sukladnosti visokorizičnih UI sustava.
- (87) Usto, ako se visokorizični UI sustav koji je sigurnosna komponenta proizvoda obuhvaćenog zakonodavstvom Unije o usklađivanju na temelju novog zakonodavnog okvira ne stavlja na tržište ili u upotrebu neovisno o proizvodu, proizvođač proizvoda definiran u tom zakonodavstvu trebao bi ispunjavati obveze dobavljača utvrđene u ovoj Uredbi, a osobito osigurati da UI sustav ugrađen u konačni proizvod ispunjava zahtjeve iz ove Uredbe.

- (88) U vrijednosnom lancu umjetne inteligencije često više strana dobavlja UI sustave, alate i usluge, ali i komponente ili procese koje dobavljač potom ugrađuje u UI sustav s različitim ciljevima, među ostalim radi treniranja modela, ponovnog treniranja modela, testiranja i evaluacije modela, integracije u softver ili drugih aspekata razvoja modela. Te strane imaju važnu ulogu u lancu vrijednosti prema dobavljaču visokorizičnog UI sustava u koji su integrirani njihovi UI sustavi, alati, usluge, komponente ili procesi te bi tom dobavljaču u pisanom obliku trebale pružiti potrebne informacije, mogućnosti, tehnički pristup i drugu pomoć na temelju općepriznatih najnovijih dostignuća kako bi dobavljač mogao u potpunosti ispuniti obveze utvrđene u ovoj Uredbi, a da se pritom ne dovedu u pitanje njihova prava intelektualnog vlasništva ili poslovne tajne.
- (89) Treće strane koje javnosti na raspolaganje stavljaju UI alate, usluge, procese ili komponente koji nisu UI modeli opće namjene ne bi trebale biti obvezne ispunjavati zahtjeve u vezi s odgovornošću duž lanca vrijednosti umjetne inteligencije, posebno prema dobavljaču koji ih je koristio ili integrirao, ako su ti UI alati, usluge, procesi ili komponente dostupni na temelju besplatne licencije za softver otvorenog koda. Razvojne programere besplatnih UI alata, usluga, procesa otvorenog koda ili komponenti koji nisu UI modeli opće namjene trebalo bi poticati da primjenjuju široko prihvaćene prakse dokumentiranja, kao što su kartice modela i podatkovne kartice kako bi se ubrzala razmjena informacija duž vrijednosnog lanca umjetne inteligencije i omogućilo promicanje pouzdanih UI sustava u Uniji.

- (90) Komisija bi mogla razviti i preporučiti dobrovoljne modele ugovornih uvjeta između dobavljača visokorizičnih UI sustava i trećih strana koji isporučuju alate, usluge, komponente ili procese koji se upotrebljavaju u visokorizičnim UI sustavima ili su u njih integrirani kako bi se olakšala suradnja duž lanca vrijednosti. Pri izradi dobrovoljnih modela ugovornih uvjeta Komisija bi trebala uzeti u obzir i moguće ugovorne zahtjeve primjenjive u određenim sektorima ili poslovnim modelima.
- (91) S obzirom na prirodu UI sustavâ i rizike za sigurnost i temeljna prava koji se potencijalno mogu povezati s njihovim korištenjem, među ostalim u pogledu potrebe da se osigura propisno praćenje učinkovitosti UI sustava u stvarnim uvjetima, primjereno je utvrditi posebne odgovornosti za subjekte koji ih uvode. Subjekti koji uvode UI sustave osobito bi trebali poduzeti primjerene tehničke i organizacijske mjere kako bi osigurali da upotrebljavaju visokorizične UI sustave u skladu s uputama za korištenje te bi, prema potrebi, trebalo predvidjeti određene druge obveze u pogledu praćenja funkcioniranja UI sustavâ i vođenja evidencije. Nadalje, subjekti koji uvode sustav trebali bi osigurati da osobe kojima je povjerena provedba uputa za korištenje i ljudskog nadzora kako je utvrđeno u ovoj Uredbi imaju potrebne kompetencije, osobito odgovarajuću razinu pismenosti, osposobljavanja i ovlasti u području umjetne inteligencije, za pravilno obavljanje tih zadaća. Tim se obvezama ne bi trebale dovoditi u pitanje druge obveze subjekata koji uvode UI sustave u pogledu visokorizičnih UI sustava na temelju prava Unije ili nacionalnog prava.

(92) Ovom se Uredbom ne dovode u pitanje obveze poslodavaca da obavijeste radnike ili njihove predstavnike ili da se savjetuju s njima na temelju prava i prakse Unije ili nacionalnog prava i prakse, uključujući Direktivu 2002/14/EZ Europskog parlamenta i Vijeća³⁹, o odlukama o stavljanju u upotrebu ili korištenju UI sustavâ. I dalje je potrebno osigurati obavješćivanje radnika i njihovih predstavnika o planiranom uvođenju visokorizičnih UI sustava na radnom mjestu ako nisu ispunjeni uvjeti za te obveze obavješćivanja ili obavješćivanja i savjetovanja iz drugih pravnih instrumenata. Nadalje, takvo pravo na obavješćivanje sporedno je i potrebno u odnosu na cilj zaštite temeljnih prava na kojem se temelji ova Uredba. Stoga bi u ovoj Uredbi trebalo utvrditi obvezu obavješćivanja u tu svrhu, a da se pritom ne utječe na postojeća prava radnika.

³⁹ Direktiva 2002/14/EZ Europskog parlamenta i Vijeća od 11. ožujka 2002. o uspostavljanju općeg okvira za obavješćivanje i savjetovanje s radnicima u Europskoj zajednici (SL L 80, 23.3.2002., str. 29.).

- (93) Iako rizici povezani s UI sustavima mogu proizlaziti iz načina na koji su ti sustavi dizajnirani, mogu biti uzrokovani i načinom na koji se oni koriste. Subjekti koji uvode visokorizične UI sustave stoga imaju ključnu ulogu u osiguravanju zaštite temeljnih prava, čime se dopunjuju obveze dobavljača pri razvoju UI sustava. Subjekti koji uvode UI sustave u najboljem su položaju da razumiju kako će se visokorizični UI sustav konkretno koristiti te stoga mogu utvrditi potencijalne znatne rizike koji nisu predviđeni u fazi razvoja, zahvaljujući preciznijem poznavanju konteksta korištenja te osoba ili skupina osoba koje bi vjerojatno bile zahvaćene, uključujući skupine ranjivih osoba. Subjekti koji uvode visokorizične UI sustave navedene u prilogu ovoj Uredbi također imaju ključnu ulogu u informiranju fizičkih osoba i trebali bi, kada donose odluke ili pomažu u donošenju odluka povezanih s fizičkim osobama, ako je primjenjivo, obavijestiti fizičke osobe da podliježu korištenju visokorizičnog UI sustava. Te informacije trebale bi obuhvaćati namjenu sustava i vrstu odluka koje donosi. Subjekt koji uvodi sustav trebao bi obavijestiti fizičke osobe i o njihovu pravu na objašnjenje predviđenom na temelju ove Uredbe. Kad je riječ o visokorizičnim UI sustavima koji se upotrebljavaju u svrhu kaznenog progona, tu bi obvezu trebalo provesti u skladu s člankom 13. Direktive (EU) 2016/680.

- (94) Svaka obrada biometrijskih podataka povezana s korištenjem UI sustava za biometrijsku identifikaciju u svrhu kaznenog progona mora biti u skladu s člankom 10. Direktive (EU) 2016/680, kojim se takva obrada dopušta samo ako je to nužno, podložno odgovarajućim zaštitnim mjerama u pogledu prava i sloboda ispitanika i ako je to dopušteno pravom Unije ili pravom države članice. Pri takvom korištenju, ako je odobreno, moraju se poštovati i načela utvrđena u članku 4. stavku 1. Direktive (EU) 2016/680, uključujući zakonitost, pravednost i transparentnost, ograničenje svrhe, točnost i ograničenje pohrane.
- (95) Ne dovodeći u pitanje primjenjivo pravo Unije, osobito Uredbu (EU) 2016/679 i Direktivu (EU) 2016/680, uzimajući u obzir intruzivnu prirodu sustava za naknadnu daljinsku biometrijsku identifikaciju, korištenje sustava za naknadnu daljinsku biometrijsku identifikaciju trebalo bi podlijeđati zaštitnim mjerama. Sustavi za naknadnu daljinsku biometrijsku identifikaciju uvijek bi se trebali upotrebljavati na način koji je proporcionalan, legitiman i nužan te stoga ciljan u smislu pojedinaca koje treba identificirati, lokacije i vremenskog opsega te se temeljiti na zatvorenom skupu podataka sa zakonito pribavljenog videozapisa. U svakom slučaju, sustavi za naknadnu daljinsku biometrijsku identifikaciju ne bi se trebali upotrebljavati u okviru kaznenog progona kako bi doveli do neselektivnog nadzora. Uvjeti za naknadnu daljinsku biometrijsku identifikaciju ni u kojem slučaju ne bi trebali biti osnova za zaobilaženje uvjeta zabrane i strogih iznimaka za daljinsku biometrijsku identifikaciju u stvarnom vremenu.

- (96) Kako bi se učinkovito osigurala zaštita temeljnih prava, subjekti koji uvode visokorizične UI sustave koji su javnopravna tijela ili privatni subjekti koji pružaju javne usluge i subjekti koji uvode određene visokorizične UI sustave navedene u prilogu ovoj Uredbi, kao što su bankarski ili osiguravateljski subjekti, trebali bi prije stavljanja tih sustava u upotrebu provesti procjenu učinka na temeljna prava. Usluge važne za pojedince koje su javne prirode mogu pružati i privatni subjekti. Privatni subjekti koji pružaju takve javne usluge povezani su sa zadaćama od javnog interesa, primjerice u područjima obrazovanja, zdravstvene skrbi, socijalnih usluga, stanovanja i sudovanja. Cilj je procjene učinka na temeljna prava da subjekt koji uvodi sustav utvrdi specifične rizike za prava pojedinaca ili skupina pojedinaca na koje bi mogao utjecati te utvrdi mjere koje se moraju poduzeti u slučaju materijalizacije tih rizika. Procjenu učinka trebala bi provesti prije uvođenja visokorizičnog UI sustava te bi je trebalo ažurirati ako subjekt koji uvodi sustav smatra da se promijenio bilo koji od relevantnih čimbenika. U procjeni učinka trebalo bi utvrditi relevantne procese subjekta koji uvodi sustav u kojima će se visokorizični UI sustav upotrebljavati u skladu sa svojom namjenom te bi ona trebala uključivati opis razdoblja i učestalosti upotrebe sustava, kao i posebnih kategorija fizičkih osoba i skupina na koje će vjerojatno utjecati u specifičnom kontekstu upotrebe.

Procjena bi trebala uključivati i utvrđivanje specifičnih rizika od štete koja bi mogla utjecati na temeljna prava tih osoba ili skupina. Pri provedbi te procjene subjekt koji uvodi UI sustav trebao bi uzeti u obzir informacije relevantne za pravilnu procjenu učinka, uključujući, ali ne ograničavajući se na informacije koje je dobavljač visokorizičnog UI sustava naveo u uputama za korištenje. S obzirom na utvrđene rizike, subjekti koji uvode sustav trebali bi utvrditi mjere koje treba poduzeti u slučaju materijalizacije tih rizika, uključujući na primjer aranžmane upravljanja u tom specifičnom kontekstu upotrebe, kao što su aranžmani za ljudski nadzor u skladu s uputama za korištenje ili postupci rješavanja pritužbi i pravne zaštite, jer bi oni mogli biti ključni za ublažavanje rizika za temeljna prava u konkretnim slučajevima korištenja. Nakon provedbe te procjene učinka subjekt koji uvodi sustav trebao bi obavijestiti relevantno tijelo za nadzor tržišta. Prema potrebi, za prikupljanje relevantnih informacija potrebnih za procjenu učinka subjekti koji uvode visokorizični UI sustav, posebno kada se UI sustavi upotrebljavaju u javnom sektoru, mogli bi u provedbu takvih procjena učinka i osmišljavanje mjera koje se moraju poduzeti u slučaju materijalizacije rizika uključiti relevantne dionike, među kojima su predstavnici skupina osoba na koje će UI sustav vjerojatno utjecati, neovisni stručnjaci i organizacije civilnog društva. Europski ured za umjetnu inteligenciju (Ured za umjetnu inteligenciju) trebao bi izraditi predložak upitnika kako bi se olakšala usklađenost i smanjilo administrativno opterećenje za subjekte koji uvode UI sustav.

- (97) Pojam UI modela opće namjene trebao bi biti jasno definiran i odvojen od pojma UI sustava kako bi se omogućila pravna sigurnost. Definicija bi se trebala temeljiti na ključnim funkcionalnim značajkama UI modela opće namjene, posebno općenitosti i sposobnosti kompetentnog obavljanja širokog raspona različitih zadaća. Ti se modeli obično treniraju s pomoću velikih količina podataka putem različitih metoda, kao što su samostalno nadzirano, nenadzirano ili podržano učenje. UI modeli opće namjene mogu se staviti na tržište na različite načine, među ostalim putem programskih knjižnica, aplikacijskih programskih sučelja, izravnim preuzimanjem ili kao fizička kopija. Ti se modeli mogu dodatno izmijeniti ili prilagoditi novim modelima. Iako su UI modeli ključne komponente UI sustava, oni sami po sebi nisu UI sustavi. UI modeli zahtijevaju dodavanje dodatnih komponenti kao što je korisničko sučelje, kako bi postali UI sustavi. UI modeli obično su integrirani u UI sustave i čine njihov sastavni dio. Ovom se Uredbom utvrđuju posebna pravila za UI modele opće namjene i UI modele opće namjene koji predstavljaju sistemske rizike, koja bi se trebala primjenjivati i kada su ti modeli integrirani u UI sustav ili su njegov dio. Trebalo bi podrazumijevati da bi se obveze dobavljača UI modela opće namjene trebale primjenjivati nakon što se ti modeli stave na tržište.

Ako dobavljač UI modela opće namjene integrira vlastiti model u vlastiti UI sustav koji je stavljen na raspolaganje na tržištu ili u upotrebu, trebalo bi smatrati da je taj model stavljen na tržište te bi se stoga obveze iz ove Uredbe koje se odnose na modele trebale nastaviti primjenjivati uz one za UI sustave. Obveze utvrđene za modele ni u kojem slučaju ne bi se trebale primjenjivati kada se vlastiti model upotrebljava za isključivo unutarnje procese koji nisu ključni za pružanje proizvoda ili usluge trećim stranama i kada to ne utječe na prava fizičkih osoba. S obzirom na njihove potencijalne znatno negativne učinke, UI modeli opće namjene sa sistemskim rizikom uvijek bi trebali podlijevati relevantnim obvezama na temelju ove Uredbe. Definicija ne bi trebala obuhvaćati UI modele koji se upotrebljavaju prije njihova stavljanja na tržište isključivo u svrhu istraživanja, razvoja i izrade prototipa. Time se ne dovodi u pitanje obveza usklađivanja s ovom Uredbom kada se, nakon takvih aktivnosti, model stavi na tržište.

- (98) Budući da bi se općenitost modela, među ostalim, mogla utvrditi i s pomoću niza parametara, trebalo bi smatrati da modeli s najmanje milijardu parametara i trenirani s pomoću velike količine podataka uz primjenu samostalnog nadzora u širokim razmjerima pokazuju znatnu razinu općenitosti i kompetentno obavljaju širok raspon različitih zadaća.
- (99) Veliki generativni UI modeli tipičan su primjer UI modela opće namjene s obzirom na to da omogućuju fleksibilnu proizvodnju sadržaja, primjerice u obliku teksta, audiozapisa, slika ili videozapisa, koji mogu lako obavljati širok raspon različitih zadaća.

- (100) Ako je UI model opće namjene integriran u UI sustav ili je njegov sastavni dio, taj bi se sustav trebao smatrati UI sustavom opće namjene ako zbog te integracije taj sustav može služiti različitim namjenama. UI sustav opće namjene može se upotrebljavati izravno ili može biti integriran u druge UI sustave.
- (101) Dobavljači UI modela opće namjene imaju posebnu ulogu i odgovornost duž vrijednosnog lanca umjetne inteligencije jer modeli koje pružaju mogu biti osnova za niz sustava niže u lancu, koje često pružaju dobavljači niže u lancu koji zahtijevaju dobro razumijevanje modela i njihovih sposobnosti kako bi omogućili integraciju takvih modela u svoje proizvode i ispunili svoje obveze na temelju ove Uredbe ili drugih uredaba. Stoga bi trebalo utvrditi razmjerne mjere transparentnosti, uključujući sastavljanje i ažuriranje dokumentacije te pružanje informacija o UI modelu opće namjene za dobavljače niže u lancu. Dobavljač UI modela opće namjene trebao bi pripremiti i ažurirati tehničku dokumentaciju kako bi je na zahtjev stavio na raspolaganje Uredu za umjetnu inteligenciju i nacionalnim nadležnim tijelima. Minimalni skup elemenata koje treba uključiti u takvu dokumentaciju trebalo bi utvrditi u specifičnim prilogima ovoj Uredbi. Komisiju bi trebalo ovlastiti da izmijeni te priloge delegiranim aktima s obzirom na tehnološki razvoj.

- (102) Softver i podaci, uključujući modele, koji se objavljuju na temelju besplatne licencije za softver otvorenog koda koja omogućuje njihovo otvoreno dijeljenje i zbog koje im korisnici mogu slobodno pristupiti, upotrebljavati ih, mijenjati i redistribuirati njih ili njihove izmijenjene verzije, mogu doprinijeti istraživanju i inovacijama na tržištu i pružiti znatne prilike za rast gospodarstva Unije. Trebalo bi razmotriti UI modele opće namjene objavljene na temelju besplatnih licencija za softver otvorenog koda kako bi se osigurala visoka razina transparentnosti i otvorenosti ako su njihovi parametri, uključujući težinske faktore, informacije o arhitekturi modela i informacije o upotrebi modela javno dostupni. Licenciju bi trebalo smatrati besplatnom licencijom za softver otvorenog koda i kada omogućuje korisnicima da pokrenu, kopiraju, distribuiraju, proučavaju, mijenjaju i poboljšavaju softver i podatke, uključujući modele, pod uvjetom da je priznat izvorni pružatelj modela i da se poštuju identični ili usporedivi uvjeti distribucije.
- (103) Besplatne UI komponente otvorenog koda obuhvaćaju softver i podatke, uključujući modele i UI modele opće namjene, alate, usluge ili procese UI sustava. Besplatne UI komponente otvorenog koda mogu se pružati različitim kanalima, uključujući njihov razvoj u otvorenim repozitorijima. Za potrebe ove Uredbe na UI komponente koje se pružaju uz naplatu ili se na drugi način monetiziraju, među ostalim i pružanjem tehničke podrške ili drugih usluga povezanih s UI komponentom, među ostalim i putem softverske platforme, ili upotrebom osobnih podataka u svrhe koje nisu isključivo povećanje sigurnosti, kompatibilnosti ili interoperabilnosti softvera, uz iznimku transakcija među mikropoduzećima, ne bi se trebale primjenjivati iznimke za besplatne UI komponente otvorenog koda. Činjenica da se UI komponente stavljaju na raspolaganje putem otvorenih repozitorija ne bi sama po sebi trebala predstavljati monetizaciju.

- (104) Dobavljači UI modela opće namjene koji se objavljuju na temelju besplatne licencije otvorenog koda i čiji su parametri, uključujući težinske faktore, informacije o arhitekturi modela i informacije o upotrebi modela, javno dostupni trebali bi podlijegati iznimkama u pogledu zahtjeva povezanih s transparentnošću nametnutih za UI modele opće namjene, osim ako se može smatrati da predstavljaju sistemski rizik, pri čemu se okolnost da je model transparentan i popraćen licencijom otvorenog koda ne bi trebala smatrati dovoljnim razlogom za isključenje ispunjavanja obveza iz ove Uredbe. U svakom slučaju, s obzirom na to da se objavom UI modelâ opće namjene na temelju besplatne licencije otvorenog koda nužno ne otkrivaju bitne informacije o skupu podataka koji se upotrebljava za treniranje ili doradu modela i o tome kako je time osigurana usklađenost s pravom o autorskom pravu, iznimka od ispunjavanja zahtjeva povezanih s transparentnošću predviđena za UI modele opće namjene ne bi se trebala odnositi na obvezu izrade sažetka o sadržaju koji se upotrebljava za treniranje modela i na obvezu uspostave politike usklađivanja s pravom Unije o autorskom pravu, posebno radi utvrđivanja i poštovanja pridržaja prava u skladu s člankom 4. stavkom 3. Direktive (EU) 2019/790 Europskog parlamenta i Vijeća⁴⁰.

⁴⁰ Direktiva (EU) 2019/790 Europskog parlamenta i Vijeća od 17. travnja 2019. o autorskom i srodnim pravima na jedinstvenom digitalnom tržištu i izmjeni direktiva 96/9/EZ i 2001/29/EZ (SL L 130, 17.5.2019., str. 92.).

- (105) UI modeli opće namjene, osobito veliki generativni UI modeli koji mogu generirati tekst, slike i druge sadržaje, pružaju jedinstvene mogućnosti za inovacije, ali i izazove za umjetnike, autore i druge kreatore te za način na koji se njihov kreativni sadržaj stvara, distribuira, upotrebljava i konzumira. Za razvoj i treniranje takvih modela potreban je pristup velikim količinama teksta, slika, videozapisa i drugih podataka. Tehnike rudarenja teksta i podataka mogu se u tom kontekstu u velikoj mjeri upotrebljavati za pronalaženje i analizu takvog sadržaja, koji može biti zaštićen autorskim pravom i povezanih pravima. Za svako korištenje sadržaja zaštićenog autorskim pravom potrebno je odobrenje nositelja prava nad tim sadržajem, osim ako se primjenjuju relevantne iznimke i ograničenja autorskog prava. Direktivom (EU) 2019/790 uvedene su iznimke i ograničenja kojima se omogućuje reproduciranje i izvlačenje djela ili drugih sadržaja u svrhu rudarenja teksta i podataka, pod određenim uvjetima. Na temelju tih pravila nositelji prava mogu odlučiti pridržati svoja prava nad svojim djelima ili drugim sadržajima kako bi spriječili rudarenje teksta i podataka, osim ako se rudarenje teksta i podataka provodi za potrebe znanstvenog istraživanja. Ako je nositelj prava izričito pridržao prava na izuzeće na primjeren način, dobavljači UI modelâ opće namjene moraju od njega dobiti odobrenje ako žele provoditi rudarenje teksta i podataka nad takvim djelima.

- (106) Dobavljači koji stavljaju UI modele opće namjene na tržište Unije trebali bi osigurati usklađenost s relevantnim obvezama iz ove Uredbe. U tu bi svrhu dobavljači UI modela opće namjene trebali uspostaviti politiku usklađivanja s pravom Unije o autorskom pravu i povezanim pravima, posebno radi utvrđivanja i poštovanja pridržaja prava koji su izrazili nositelji prava u skladu s člankom 4. stavkom 3. Direktive (EU) 2019/790. Svaki dobavljač koji na tržište Unije stavlja UI model opće namjene trebao bi ispunjavati tu obvezu, bez obzira na jurisdikciju u kojoj se odvijaju radnje povezane s autorskim pravima na kojima se temelji treniranje tih UI modela opće namjene. To je potrebno kako bi se osigurali jednaki uvjeti među dobavljačima UI modela opće namjene prema kojima nijedan dobavljač ne bi trebao moći steći konkurentsku prednost na tržištu Unije primjenom nižih standarda autorskih prava od onih koji su predviđeni u Uniji.

- (107) Kako bi se povećala transparentnost podataka koji se upotrebljavaju u prethodnom treniranju i treniranju UI modela opće namjene, uključujući tekst i podatke zaštićene autorskim pravom, primjereno je da dobavljači takvih modela sastave i objave dovoljno detaljan sažetak sadržaja koji se upotrebljava za treniranje UI modela opće namjene. Uzimajući u obzir potrebu za zaštitom poslovnih tajni i povjerljivih poslovnih informacija, taj bi sažetak trebao biti općenito sveobuhvatan u svojem opsegu, a ne tehnički detaljan, kako bi se strankama s legitimnim interesima, uključujući nositelje autorskih prava, olakšalo ostvarivanje i izvršavanje njihovih prava na temelju prava Unije, na primjer navođenjem glavnih zbirki ili skupova podataka koji su upotrijebljeni pri treniranju modela, kao što su velike privatne ili javne baze podataka ili arhive podataka, te pružanjem opisnog objašnjenja o drugim korištenim izvorima podataka. Primjereno je da Ured za umjetnu inteligenciju dostavi predložak sažetka, koji bi trebao biti jednostavan, djelotvoran i omogućiti dobavljaču da dostavi traženi sažetak u opisnom obliku.
- (108) Kad je riječ o obvezama nametnutima dobavljačima UI modela opće namjene da uspostave politiku usklađivanja s pravom Unije o autorskom pravu i objave sažetak sadržaja koji se upotrebljava za treniranje, Ured za umjetnu inteligenciju trebao bi pratiti je li dobavljač ispunio te obveze bez provjere ili pojedinačnog ocjenjivanja podataka korištenih za treniranje u pogledu usklađenosti s autorskim pravom. Ova Uredba ne utječe na izvršavanje pravila o autorskom pravu kako su predviđena pravom Unije.

- (109) Usklađenost s obvezama koje se primjenjuju na dobavljače UI modela opće namjene trebala bi biti razmjerna i primjerena vrsti dobavljača modela, isključujući potrebu za usklađenosti za osobe koje razvijaju ili upotrebljavaju modele u neprofesionalne ili znanstveno-istraživačke svrhe, no koje bi ipak trebalo poticati da dobrovoljno ispune te zahtjeve. Ne dovodeći u pitanje pravo Unije o autorskom pravu, pri ispunjavanju tih obveza trebalo bi uzeti u obzir veličinu dobavljača i omogućiti pojednostavnjene načine usklađivanja za MSP-ove, uključujući *start-up* poduzeća, koji ne bi trebali predstavljati pretjerani trošak niti obeshrabrivati korištenje takvih modela. U slučaju izmjene ili dorade modela, obveze dobavljača UI modela opće namjene trebale bi biti ograničene na tu izmjenu ili doradu, na primjer dopunjavanjem već postojeće tehničke dokumentacije informacijama o izmjenama, uključujući nove izvore podataka za treniranje, kako bi se ispunile obveze u pogledu vrijednosnog lanca predviđene u ovoj Uredbi.

- (110) UI modeli opće namjene mogli bi predstavljati sistemske rizike koji uključuju, ali nisu ograničeni na, sve stvarne ili razumno predvidljive negativne učinke povezane s velikim nesrećama, poremećajima u kritičnim sektorima i ozbiljnim posljedicama za javno zdravlje i sigurnost; sve stvarne ili razumno predvidljive negativne učinke na demokratske procese, javnu i gospodarsku sigurnost; širenje nezakonitog, lažnog ili diskriminirajućeg sadržaja. Trebalo bi razumjeti da se sistemski rizici povećavaju s kapacitetom i dosegom modela, da se mogu pojaviti tijekom cijelog životnog ciklusa modela i da na njih utječu uvjeti pogrešne upotrebe, pouzdanost modela, pravednost modela i sigurnost modela, razinu autonomije modela, njegov pristup alatima, novi ili kombinirani modaliteti, strategije objave i distribucije, potencijal za uklanjanje zaštitnih mehanizama i drugi čimbenici. Konkretno, u međunarodnim pristupima dosad je utvrđeno da je potrebno posvetiti pozornost rizicima od moguće namjerne pogrešne upotrebe ili nenamjernih problemima u kontroli koji se odnose na usklađivanje s ljudskom namjerom; kemijskim, biološkim, radiološkim i nuklearnim rizicima, kao što su načini na koje se mogu smanjiti prepreke za pristup, uključujući za razvoj oružja, nabavu njihova dizajna ili njihovu upotrebu; ofenzivnim kibernetičkim sposobnostima, kao što su načini omogućavanja otkrivanja, iskorištavanja ili operativne upotrebe slabih točaka; učincima interakcije i upotrebe alata, uključujući, na primjer, sposobnost kontrole fizičkih sustava i ometanja kritične infrastrukture; rizicima povezanim s modelima koji izrađuju svoje kopije ili se „samorepliciraju” ili treniraju druge modele; načinima na koje modeli mogu dovesti do štetne pristranosti i diskriminacije uz rizike za pojedince, zajednice ili društva; olakšavanju širenja dezinformacija ili ugrožavanju privatnosti prijetnjama demokratskim vrijednostima i ljudskim pravima; riziku od toga da bi određeni događaj mogao dovesti do lančane reakcije sa znatnim negativnim učincima koji bi mogli utjecati na cijeli grad, cijelu aktivnost u nekoj domeni ili cijelu zajednicu.

- (111) Primjereno je uspostaviti metodologiju za klasifikaciju UI modela opće namjene kao UI modela opće namjene sa sistemskim rizicima. Budući da sistemski rizici proizlaze iz posebno visokih sposobnosti, trebalo bi smatrati da UI model opće namjene predstavlja sistemske rizike ako ima sposobnosti visokog učinka, koje se ocjenjuje na temelju odgovarajućih tehničkih alata i metodologija, ili ako zbog svojeg dosega znatno utječe na unutarnje tržište. Sposobnosti visokog učinka kod UI modela opće namjene znači sposobnosti koje odgovaraju sposobnostima zabilježenima kod najnaprednijih UI modela opće namjene ili ih nadilaze. Cijeli raspon sposobnosti modela mogao bi se bolje razumjeti nakon njegova stavljanja na tržište ili pri interakciji dobavljača s modelom. U skladu s najnovijim dostignućima u trenutku stupanja na snagu ove Uredbe, kumulativna količina računanja korištena za treniranje UI modela opće namjene iskazana brojem matematičkih operacija nad brojevima s pomičnim zarezom jedna je od relevantnih približnih vrijednosti za sposobnosti modela. Kumulativna količina računanja korištena za treniranje uključuje računanje korišteno u svim aktivnostima i metode namijenjene poboljšanju sposobnosti modela prije uvođenja, kao što su prethodno treniranje, generiranje sintetičkih podataka i dorada. Stoga bi trebalo utvrditi početni prag za matematičke operacije nad brojevima s pomičnim zarezom, koji, ako ga UI model opće namjene dosegne, dovodi do pretpostavke da je riječ o UI modelu opće namjene sa sistemskim rizicima. Taj bi prag trebalo s vremenom prilagoditi kako bi odražavao tehnološke i industrijske promjene, kao što su algoritamska poboljšanja ili povećana učinkovitost hardvera, te bi ga trebalo dopuniti referentnim vrijednostima i pokazateljima sposobnosti modela.

U tu bi svrhu Ured za umjetnu inteligenciju trebao surađivati sa znanstvenom zajednicom, strukom, civilnim društvom i drugim stručnjacima. Pragovi, kao i alati i referentne vrijednosti za procjenu sposobnosti visokog učinka, trebali bi u velikoj mjeri predvidjeti općenitost, sposobnosti i povezani sistemski rizik UI modela opće namjene te bi se njima moglo uzeti u obzir način na koji će se model staviti na tržište ili broj korisnika na koji bi mogao utjecati. Kako bi se taj sustav dopunio, Komisija bi trebala moći donijeti pojedinačne odluke kojima se UI model opće namjene određuje kao UI model opće namjene sa sistemskim rizikom ako se utvrdi da takav model ima sposobnosti ili učinak jednakovrijedan onima koji su obuhvaćeni utvrđenim pragom. Ta bi se odluka trebala donijeti na temelju opće procjene kriterijâ za određivanje UI modela opće namjene sa sistemskim rizikom navedenih u prilogu ovoj Uredbi, kao što su kvaliteta ili veličina skupa podataka za treniranje, broj poslovnih i krajnjih korisnika, njihovi ulazni i izlazni modaliteti, razina autonomije i skalabilnosti ili alati kojima ima pristup. Na obrazloženi zahtjev dobavljača čiji je model određen kao UI model opće namjene sa sistemskim rizikom Komisija bi takav zahtjev trebala uzeti u obzir i može odlučiti ponovno ocijeniti može li se i dalje smatrati da UI model opće namjene predstavlja sistemske rizike.

- (112) Također je potrebno pojasniti proceduru za klasifikaciju UI modela opće namjene kao UI modela opće namjene sa sistemskim rizicima. Za UI model opće namjene koji je dosegao primjenjivi prag za sposobnosti visokog učinka trebalo bi se pretpostaviti da je riječ o UI modelu opće namjene sa sistemskim rizikom. Dobavljač bi trebao obavijestiti Ured za umjetnu inteligenciju najkasnije dva tjedna nakon što su zahtjevi ispunjeni ili nakon što postane poznato da će UI model opće namjene ispunjavati zahtjeve koji dovode do te pretpostavke. To je posebno važno u odnosu na prag matematičkih operacija nad brojevima s pomičnim zarezom jer je za treniranje UI modela opće namjene potrebno znatno planiranje koje uključuje prethodnu dodjelu računalnih resursa te stoga dobavljači UI modela opće namjene mogu znati bi li njihov model dosegnuo prag prije završetka postupka treniranja. U kontekstu te obavijesti dobavljač bi trebao moći dokazati da, zbog posebnih značajki UI modela opće namjene, taj model iznimno ne predstavlja sistemske rizike te da ga stoga ne bi trebalo klasificirati kao UI model opće namjene sa sistemskim rizicima. Te su informacije vrijedne Uredu za umjetnu inteligenciju kako bi predvidio stavljanje na tržište UI modela opće namjene sa sistemskim rizicima, a dobavljači mogu rano početi surađivati s Uredom za umjetnu inteligenciju. Te su informacije posebno važne u pogledu UI modela opće namjene koji se planiraju objaviti kao otvoreni kod, s obzirom na to da bi nakon objave modela otvorenog koda moglo biti teže provesti potrebne mjere za osiguravanje usklađenosti s obvezama iz ove Uredbe.

- (113) Ako Komisija sazna da UI model opće namjene ispunjava zahtjeve da ga se klasificira kao UI model opće namjene sa sistemskim rizikom, a prethodno nije bio poznat ili o njemu relevantni dobavljač nije obavijestio Komisiju, Komisija bi trebala biti ovlaštena odrediti ga kao takvoga. Sustav kvalificiranih upozorenja trebao bi osigurati da znanstveno povjerenstvo obavijesti Ured za umjetnu inteligenciju o UI modelima opće namjene koje bi potencijalno trebalo klasificirati kao UI modele opće namjene sa sistemskim rizikom, kao i o aktivnostima praćenja Ureda za umjetnu inteligenciju.
- (114) Dobavljači UI modela opće namjene koji predstavljaju sistemske rizike trebali bi, uz obveze predviđene za dobavljače UI modela opće namjene, podlijegati obvezama usmjerenima na utvrđivanje i ublažavanje tih rizika i osiguravanje odgovarajuće razine kibernetičkosigurnosne zaštite, bez obzira na to pružaju li se kao samostalni model ili su ugrađeni u UI sustav ili proizvod. Kako bi se postigli ti ciljevi, ovom bi se Uredbom od dobavljača trebalo zahtijevati da provedu potrebne evaluacije modela, posebno prije njihova prvog stavljanja na tržište, uključujući provođenje i dokumentiranje neprijateljskog testiranja modela, također, prema potrebi, unutarnjim testiranjem ili neovisnim vanjskim testiranjem. Osim toga, dobavljači UI modela opće namjene sa sistemskim rizicima trebali bi kontinuirano procjenjivati i ublažavati sistemske rizike, među ostalim i, primjerice, uspostavom politika upravljanja rizikom, kao što su postupci odgovornosti i upravljanja, provedbom praćenja nakon stavljanja na tržište, poduzimanjem odgovarajućih mjera tijekom cijelog životnog ciklusa modela i suradnjom s relevantnim akterima duž lanca vrijednosti umjetne inteligencije.

- (115) Dobavljači UI modela opće namjene sa sistemskim rizicima trebali bi procijeniti i ublažiti moguće sistemske rizike. Ako, unatoč nastojanjima da se utvrde i spriječe rizici povezani s UI modelom opće namjene koji bi mogao predstavljati sistemske rizike, razvoj ili korištenje modela uzrokuju ozbiljan incident, dobavljač UI modela opće namjene trebao bi bez nepotrebne odgode pratiti incident i izvješćivati Komisiju i nacionalna nadležna tijela o svim relevantnim informacijama i mogućim korektivnim mjerama. Nadalje, dobavljači bi trebali osigurati odgovarajuću razinu kibernetičkosigurnosne zaštite modela i njegove fizičke infrastrukture, prema potrebi, tijekom cijelog životnog ciklusa modela.
- Kibernetičkosigurnosnom zaštitom koja je povezana sa sistemskim rizicima povezanim sa zlonamjernom upotrebom ili napadima trebalo bi na odgovarajući način uzeti u obzir slučajno curenje iz modela, neovlaštena objavljivanja, zaobilaženje sigurnosnih mjera i obranu od kibernetičkih napada, neovlaštenog pristupa ili krađe modela. Ta bi se zaštita mogla olakšati osiguravanjem težinskih faktora modela, algoritama, poslužitelja i skupova podataka, primjerice mjerama operativne sigurnosti za informacijsku sigurnost, posebnim kibernetičkosigurnosnim politikama, odgovarajućim tehničkim i utvrđenim rješenjima te kontrolama kibernetičkog i fizičkog pristupa, koji su primjereni relevantnim okolnostima i uključenim rizicima.

- (116) Ured za umjetnu inteligenciju trebao bi poticati i olakšati izradu, preispitivanje i prilagodbu kodeksâ prakse, uzimajući u obzir međunarodne pristupe. Svi dobavljači UI modela opće namjene mogli bi biti pozvani na sudjelovanje. Kako bi se osiguralo da se kodeksima prakse odražavaju najnovija dostignuća i na odgovarajući način uzimaju u obzir različite perspektive, Ured za umjetnu inteligenciju trebao bi surađivati s relevantnim nacionalnim nadležnim tijelima te bi se, prema potrebi, mogao savjetovati s organizacijama civilnog društva i drugim relevantnim dionicima i stručnjacima, uključujući znanstveno povjerenstvo, radi izrade takvih kodeksa. Kodeksi prakse trebali bi obuhvaćati obveze dobavljača UI modela opće namjene i UI modela opće namjene koji predstavljaju sistemske rizike. Osim toga, kad je riječ o sistemskim rizicima, kodeksi prakse trebali bi pomoći u uspostavi taksonomije vrste i prirode sistemskih rizika na razini Unije, uključujući njihove izvore. Kodeksi prakse trebali bi biti usmjereni i na posebne mjere procjene i ublažavanja rizika.

- (117) Kodeksi prakse trebali bi biti središnji alat za pravilno ispunjavanje obveza predviđenih na temelju ove Uredbe za dobavljače UI modela opće namjene. Dobavljači bi se trebali moći osloniti na kodekse prakse kako bi dokazali ispunjavanje obveza. Komisija provedbenim aktima može odlučiti odobriti kodeks prakse i učiniti ga općenito valjanim u Uniji ili, alternativno, utvrditi zajednička pravila za provedbu relevantnih obveza ako do početka primjene ove Uredbe kodeks prakse ne može biti dovršen ili ga Ured za umjetnu inteligenciju ne smatra adekvatnim. Nakon što se usklađena norma objavi i Ured za umjetnu inteligenciju ocijeni je prikladnom za obuhvaćanje relevantnih obveza, ispunjavanje europske usklađene norme dobavljačima bi trebalo omogućiti pretpostavku sukladnosti. Nadalje, dobavljači UI modela opće namjene trebali bi moći dokazati ispunjavanje obveza s pomoću alternativnih odgovarajućih sredstava ako kodeksi prakse ili usklađene norme nisu dostupni ili ako odluče da se neće oslanjati na njih.

- (118) Ovom se Uredbom reguliraju UI sustavi i modeli uvođenjem određenih zahtjeva i obveza za relevantne aktere na tržištu koji ih stavljaju na tržište ili u upotrebu ili ih upotrebljavaju u Uniji, čime se dopunjuju obveze pružatelja usluga posredovanja koji takve sustave ili modele ugrađuju u svoje usluge regulirane Uredbom (EU) 2022/2065. U mjeri u kojoj su takvi sustavi ili modeli ugrađeni u određene vrlo velike internetske platforme ili vrlo velike internetske tražilice, na njih se primjenjuje okvir za upravljanje rizicima predviđen u Uredbi (EU) 2022/2065. Stoga bi trebalo pretpostaviti da su odgovarajuće obveze iz ove Uredbe ispunjene, osim ako se u takvim modelima pojave znatni sistemski rizici koji nisu obuhvaćeni Uredbom (EU) 2022/2065. Unutar tog okvira pružatelji vrlo velikih internetskih platformi i vrlo velikih internetskih tražilica obvezni su procijeniti potencijalne sistemske rizike koji proizlaze iz dizajna, funkcioniranja i korištenja njihovih usluga, uključujući način na koji dizajn algoritamskih sustava koji se upotrebljavaju u usluzi može doprinijeti takvim rizicima, kao i sistemske rizike koji proizlaze iz mogućih pogrešnih upotreba. Ti su pružatelji također obvezni poduzeti odgovarajuće mjere za ublažavanje rizika za temeljna prava.

- (119) S obzirom na brz tempo inovacija i tehnološki razvoj digitalnih usluga u području primjene različitih instrumenata prava Unije, posebno imajući na umu upotrebu i percepciju njihovih primatelja, UI sustavi koji podliježu ovoj Uredbi mogu se pružati kao usluge posredovanja ili njihovi dijelovi u smislu Uredbe (EU) 2022/2065, koje bi trebalo tumačiti na tehnološki neutralan način. Na primjer, UI sustavi mogu se upotrebljavati za pružanje internetskih tražilica, posebno u mjeri u kojoj UI sustav, kao što je internetski chatbot, u načelu pretražuje sve internetske stranice, zatim uključuje rezultate u svoje postojeće znanje i upotrebljava nadopunjeno znanje kako bi generirao jedan izlazni rezultat koji objedinjuje različite izvore informacija.
- (120) Nadalje, obveze propisane u ovoj Uredbi za dobavljače i za subjekte koji uvode određene UI sustave kako bi se omogućilo prepoznavanje i otkrivanje umjetno stvorenih ili manipuliranih izlaznih rezultata tih sustava posebno su relevantne za olakšavanje djelotvorne provedbe Uredbe (EU) 2022/2065. To se posebno odnosi na obveze pružatelja vrlo velikih internetskih platformi ili vrlo velikih internetskih tražilica da utvrde i ublaže sistemske rizike koji mogu proizaći iz širenja umjetno stvorenog ili manipuliranog sadržaja, posebno rizik od stvarnih ili predvidljivih negativnih učinaka na demokratske procese, građanski diskurs i izborne procese, među ostalim dezinformiranjem.

- (121) Normizacija bi trebala imati ključnu ulogu u pružanju tehničkih rješenja dobavljačima kako bi se osigurala usklađenost s ovom Uredbom, u skladu s najnovijim dostignućima, kako bi se promicale inovacije te konkurentnost i rast na jedinstvenom tržištu.
- Poštovanje usklađenih normi kako su definirane u članku 2. točki 1. podtočki (c) Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća⁴¹, za koje se obično očekuje da odražavaju najnovija dostignuća, trebalo bi biti sredstvo kojim će dobavljači dokazivati sukladnost sa zahtjevima ove Uredbe. Stoga bi u skladu s člancima 5. i 6. Uredbe (EU) br. 1025/2012 trebalo poticati uravnoteženu zastupljenost interesa koja uključuje sve relevantne dionike u razvoju normi, posebno MSP-ove, organizacije potrošača te dionike u području okoliša i socijalne dionike. Kako bi se olakšala sukladnost, Komisija bi trebala izdati zahtjeve za normizaciju bez nepotrebne odgode. Pri izradi zahtjeva za normizaciju Komisija bi se trebala savjetovati sa savjetodavnim forumom i Vijećem za umjetnu inteligenciju kako bi obuhvatila relevantno stručno znanje. Međutim, u nedostatku relevantnih upućivanja na usklađene norme, Komisija bi trebala moći provedbenim aktima i nakon savjetovanja sa savjetodavnim forumom utvrditi zajedničke specifikacije za određene zahtjeve na temelju ove Uredbe.

⁴¹ Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

Zajednička specifikacija trebala bi biti iznimno zamjensko rješenje kako bi se dobavljaču olakšalo ispunjavanje zahtjeva iz ove Uredbe kada nijedna europska organizacija za normizaciju nije prihvatila zahtjev za normizaciju ili kada se relevantnim usklađenim normama u nedovoljnoj mjeri rješavaju problemi u području temeljnih prava ili kada usklađene norme nisu u skladu sa zahtjevom ili kada dođe do kašnjenja u donošenju odgovarajuće usklađene norme. Ako je takvo kašnjenje u donošenju usklađene norme posljedica tehničke složenosti te norme, Komisija bi to trebala razmotriti prije razmatranja utvrđivanja zajedničkih specifikacija. Pri izradi zajedničkih specifikacija Komisiju se potiče na suradnju s međunarodnim partnerima i međunarodnim tijelima za normizaciju.

- (122) Ne dovodeći u pitanje upotrebu usklađenih normi i zajedničkih specifikacija, primjereno je da se za dobavljače visokorizičnog UI sustava koji je treniran i testiran na podacima koji odražavaju specifično zemljopisno, bihevioralno, kontekstualno ili funkcionalno okružje u kojem se UI sustav namjerava upotrebljavati smatra da su sukladni s relevantnom mjerom predviđenom u zahtjevu u pogledu upravljanja podacima utvrđenom u ovoj Uredbi. Ne dovodeći u pitanje zahtjeve koji se odnose na otpornost i točnost utvrđene u ovoj Uredbi, u skladu s člankom 54. stavkom 3. Uredbe (EU) 2019/881, za visokorizične UI sustave koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibernetičke sigurnosti na temelju te uredbe i na koje su objavljena upućivanja u *Službenom listu Europske unije* trebalo bi pretpostaviti da ispunjavaju kibernetičkosigurnosne zahtjeve iz ove Uredbe u mjeri u kojoj certifikat o kibernetičkoj sigurnosti ili izjava o sukladnosti ili njihovi dijelovi obuhvaćaju kibernetičkosigurnosne zahtjeve iz ove Uredbe. Time se i dalje ne dovodi u pitanje dobrovoljna priroda tog programa kibernetičke sigurnosti.
- (123) Kako bi se osigurala visoka razina pouzdanosti visokorizičnih UI sustava, ti bi sustavi trebali podlijevati ocjenjivanju sukladnosti prije njihova stavljanja na tržište ili u upotrebu.

- (124) Kako bi se opterećenje za operatere svelo na najmanju moguću mjeru i izbjeglo moguće udvostručavanje, za visokorizične UI sustave povezane s proizvodima koji su obuhvaćeni postojećim zakonodavstvom Unije o usklađivanju na temelju novog zakonodavnog okvira, usklađenost tih UI sustava sa zahtjevima ove Uredbe trebala bi se ocjenjivati u okviru ocjenjivanja sukladnosti koje je već predviđeno u tom pravu. Primjenjivost zahtjevâ ove Uredbe stoga ne bi trebala utjecati na specifičnu logiku, metodologiju ili opću strukturu ocjenjivanja sukladnosti na temelju relevantnog zakonodavstva Unije o usklađivanju.
- (125) S obzirom na složenost visokorizičnih UI sustava i s njima povezane rizike, važno je razviti odgovarajući sustav postupka ocjenjivanja sukladnosti visokorizičnih UI sustava koji uključuje prijavljena tijela, tzv. ocjenjivanje sukladnosti koje provodi treća strana. Međutim, s obzirom na trenutačno iskustvo profesionalnih certifikatora proizvoda prije stavljanja na tržište u području sigurnosti proizvoda i različitu prirodu uključenih rizika, primjereno je, barem u početnoj fazi primjene ove Uredbe, ograničiti područje primjene ocjenjivanja sukladnosti visokorizičnih UI sustava koje provodi treća strana, osim za one sustave koji su povezani s proizvodima. Stoga bi ocjenjivanje sukladnosti takvih sustava u pravilu trebao provoditi dobavljač na vlastitu odgovornost, uz jedinu iznimku UI sustava namijenjenih za biometriju.

- (126) Za ocjenjivanje sukladnosti koje provodi treća strana kada je to potrebno, nacionalna nadležna tijela trebala bi na temelju ove Uredbe prijavljivati prijavljena tijela, pod uvjetom da ispunjavaju niz zahtjeva, ponajprije u pogledu neovisnosti, kompetentnosti, nepostojanja sukoba interesa i odgovarajućih kibernetičkosigurnosnih zahtjeva. Nacionalna nadležna tijela trebala bi Komisiji i drugim državama članicama slati obavijesti o prijavljivanju tih tijela pomoću alata za elektroničko prijavljivanje koji je razvila i kojim upravlja Komisija u skladu s člankom R23. Priloga I. Odluci br. 768/2008/EZ.
- (127) U skladu s obvezama Unije na temelju Sporazuma Svjetske trgovinske organizacije o tehničkim preprekama u trgovini primjereno je olakšati uzajamno prihvaćanje rezultata ocjenjivanja sukladnosti koje su proizvela nadležna tijela za ocjenjivanje sukladnosti, bez obzira na to na kojem području imaju poslovni nastan, pod uvjetom da ta tijela za ocjenjivanje sukladnosti osnovana na temelju prava treće zemlje ispunjavaju primjenjive zahtjeve ove Uredbe i da je Unija sklopila odgovarajući sporazum. U tom kontekstu Komisija bi trebala aktivno istražiti moguće međunarodne instrumente u tu svrhu, a posebno nastojati sklopiti sporazume o uzajamnom priznavanju s trećim zemljama.

- (128) U skladu sa zajednički utvrđenim pojmom znatne izmjene za proizvode regulirane zakonodavstvom Unije o usklađivanju primjereno je da se svaki put kad dođe do promjene koja može utjecati na usklađenost visokorizičnog UI sustava s ovom Uredbom (npr. promjena operativnog sustava ili softverske arhitekture) ili kad se promijeni namjena sustava, taj UI sustav smatra novim UI sustavom koji bi trebao proći novo ocjenjivanje sukladnosti. Međutim, promjene algoritma i učinkovitosti UI sustava koji nakon stavljanja na tržište ili u upotrebu nastavljaju „učiti”, odnosno automatski prilagođavati način izvršavanja funkcija, ne bi trebale predstavljati znatnu izmjenu, pod uvjetom da je te promjene unaprijed odredio dobavljač i da su ocijenjene u trenutku ocjenjivanja sukladnosti.
- (129) Visokorizični UI sustavi trebali bi nositi oznaku CE koja upućuje na njihovu sukladnost s ovom Uredbom kako bi se mogli slobodno kretati na unutarnjem tržištu. Kad je riječ o visokorizičnim UI sustavima ugrađenima u proizvod, fizička oznaka CE trebala bi biti pričvršćena na njih te se može dopuniti digitalnom oznakom CE. Za visokorizične UI sustave koji se pružaju samo digitalno trebalo bi upotrebljavati digitalnu oznaku CE. Države članice ne bi trebale stvarati neopravdane zapreke stavljanju na tržište ili u upotrebu visokorizičnih UI sustava koji ispunjavaju zahtjeve utvrđene u ovoj Uredbi i nose oznaku CE.

- (130) Po određenim uvjetima brza dostupnost inovativnih tehnologija može biti ključna za zdravlje i sigurnost osoba, zaštitu okoliša i klimatske promjene te za društvo u cjelini. Stoga je primjereno da bi zbog iznimnih razloga povezanih s javnom sigurnošću ili zaštitom života i zdravlja fizičkih osoba, zaštitom okoliša i ključne industrijske i infrastrukturne imovine, tijela za nadzor tržišta mogla odobriti stavljanje na tržište ili u upotrebu UI sustava za koje nije proveden postupak ocjenjivanja sukladnosti. U propisno opravdanim situacijama, kako je predviđeno u ovoj Uredbi, tijela kaznenog progona ili tijela civilne zaštite mogu staviti u upotrebu određeni visokorizični UI sustav bez odobrenja tijela za nadzor tržišta, pod uvjetom da se takvo odobrenje zatraži tijekom ili nakon korištenja bez nepotrebne odgode.
- (131) Kako bi se olakšao rad Komisije i država članica u području umjetne inteligencije i povećala transparentnost prema javnosti, od dobavljača visokorizičnih UI sustava koji nisu povezani s proizvodima obuhvaćenima područjem primjene relevantnog postojećeg zakonodavstva Unije o usklađivanju, kao i dobavljača koji smatraju da pojedini UI sustav naveden u primjerima visokorizične upotrebe iz priloga ovoj Uredbi nije visokorizičan na temelju odstupanja, trebalo bi zahtijevati da sebe i informacije o svojem UI sustavu registriraju u bazi podataka EU-a, koju će uspostaviti i kojom će upravljati Komisija. Prije upotrebi UI sustava navedenog u primjerima visokorizične upotrebe iz priloga ovoj Uredbi subjekti koji uvode visokorizične UI sustave koji su tijela javne vlasti, javne agencije ili javna tijela trebali bi se registrirati u takvoj bazi podataka i odabrati sustav koji namjeravaju upotrebljavati.

Ostali subjekti koji uvode sustav trebali bi imati pravo to učiniti dobrovoljno. Taj dio baze podataka EU-a trebao bi biti javno dostupan, besplatno, a informacije bi trebale biti lako dostupne, razumljive i strojno čitljive. Baza podataka EU-a trebala bi biti prilagođena korisnicima, na primjer pružanjem funkcija pretraživanja, među ostalim s pomoću ključnih riječi, čime bi se široj javnosti omogućio pronalazak relevantnih informacija koje treba dostaviti nakon registracije visokorizičnih UI sustava i relevantnih informacija o slučaju upotrebe visokorizičnih UI sustava navedenih u prilogu ovoj Uredbi, kojima visokorizični UI sustavi odgovaraju. Svaka bitna izmjena visokorizičnih UI sustava također bi se trebala registrirati u bazi podataka EU-a. Kad je riječ o visokorizičnim UI sustavima u područjima kaznenog progona ili migracija, azila i upravljanja nadzorom državne granice, obveze registracije trebale bi se ispuniti u sigurnom dijelu baze podataka EU-a koji nije javan. Pristup sigurnom dijelu koji nije javan trebao bi biti strogo ograničen na Komisiju i tijela za nadzor tržišta na čiju se državu odnosi taj dio baze podataka. Visokorizične UI sustave u području kritične infrastrukture trebalo bi registrirati samo na nacionalnoj razini. Komisija bi trebala biti voditelj obrade baze podataka EU-a, u skladu s Uredbom 2018/1725. Kako bi baza podataka EU-a bila posve funkcionalna od puštanja u rad, postupak njezina uspostavljanja trebao bi uključivati razvoj funkcionalnih specifikacija, što je zadaća Komisije, te neovisno revizorsko izvješće. Komisija bi pri obavljanju svojih zadaća voditelja obrade podataka u bazi podataka EU-a trebala uzeti u obzir rizike povezane s kibernetičkom sigurnosti. Kako bi se maksimalno povećale dostupnost i upotreba baze podataka EU-a u javnosti, baza podataka EU-a, uključujući podatke koji su u njoj dostupni, trebala bi ispunjavati zahtjeve iz Direktive (EU) 2019/882.

- (132) Kod određenih UI sustava namijenjenih interakciji s fizičkim osobama ili generiranju sadržaja mogu postojati posebni rizici u pogledu lažnog predstavljanja ili obmanjivanja, bez obzira na to smatraju li se visokorizičnima. Korištenje tih sustava stoga bi u određenim okolnostima trebalo podlijegati posebnim obvezama u pogledu transparentnosti, ne dovodeći u pitanje zahtjeve i obveze za visokorizične UI sustave, i ciljanim iznimkama kako bi se uzela u obzir posebna potreba kaznenog progona. Osobito bi fizičke osobe trebalo obavijestiti o tome da su u interakciji s UI sustavom, osim ako je to očito sa stajališta razmjerno dobro informirane, pronicljive i oprezne fizičke osobe, uzimajući u obzir okolnosti i kontekst upotrebe. Pri provedbi te obveze trebalo bi uzeti u obzir karakteristike fizičkih osoba koje pripadaju skupinama ranjivih osoba zbog svoje dobi ili invaliditeta u mjeri u kojoj je UI sustav namijenjen i interakciji s tim skupinama. Nadalje, fizičke osobe trebalo bi obavijestiti kada su izložene UI sustavima koji obradom njihovih biometrijskih podataka mogu identificirati emocije, izvoditi zaključke o njihovim emocijama ili namjerama ili te osobe razvrstati u određene kategorije. Te se određene kategorije mogu odnositi na aspekte kao što su spol, dob, boja kose, boja očiju, tetovaže, osobna obilježja, etničko podrijetlo, osobne preferencije i interesi. Takve informacije i obavijesti trebale bi se davati u oblicima koji su pristupačni osobama s invaliditetom.

- (133) Različiti UI sustavi mogu generirati velike količine sintetičkog sadržaja koji ljudima postaje sve teže razlikovati od autentičnog sadržaja koji je stvorio čovjek. Široka dostupnost i sve veće sposobnosti tih sustava znatno utječu na integritet informacijskog ekosustava i povjerenje u njega, pri čemu dovode do novih rizika od široko rasprostranjenih dezinformacija i manipulacije, prijevara, lažnog predstavljanja i obmanjivanja potrošača. S obzirom na te učinke, brz tehnološki razvoj i potrebu za novim metodama i tehnikama za praćenje podrijetla informacija, primjereno je od dobavljača tih sustava zahtijevati da ugrade tehnička rješenja koja omogućuju označivanje u strojno čitljivom formatu i prepoznavanje toga da je izlazni rezultat generirao ili je njime manipulirao UI sustav, a ne čovjek. Takve tehnike i metode trebale bi biti dovoljno pouzdane, interoperabilne, učinkovite i pouzdane u mjeri u kojoj je to tehnički izvedivo, uzimajući u obzir raspoložive tehnike ili kombinaciju takvih tehnika, kao što su vođeni žigovi, identifikacija metapodataka, kriptografske metode za dokazivanje podrijetla i autentičnosti sadržaja, metode evidentiranja, otisci prstiju ili druge tehnike, ovisno o slučaju. Pri provedbi te obveze dobavljači bi trebali uzeti u obzir i posebnosti i ograničenja različitih vrsta sadržaja te relevantna tehnološka i tržišna kretanja u tom području, kako se odražavaju u općepriznatim najnovijim dostignućima. Takve tehnike i metode mogu se primijeniti na razini UI sustava ili na razini UI modela, uključujući UI modele opće namjene koji generiraju sadržaj, čime se dobavljaču UI sustava niže u lancu olakšava ispunjavanje te obveze. Kako bi i dalje bila razmjerna, primjereno je predvidjeti da ta obveza označivanja ne bi trebala obuhvaćati UI sustave koji prvenstveno imaju pomoćnu funkciju za standardno uređivanje ili UI sustave koji bitno ne mijenjaju ulazne podatke koje pruža subjekt koji uvodi sustav ili njihovu semantiku.

- (134) Uz tehnička rješenja koja primjenjuju dobavljači sustava, subjekti koji uvode UI sustav, koji upotrebljavaju UI sustav za generiranje slikovnog sadržaja, audiosadržaja ili videosadržaja u kojem postoji znatna sličnost s postojećim osobama, predmetima, mjestima, subjektima ili događajima i koji bi se nekome lažno činio vjerodostojnim ili istinitim (uvjerljiv krivotvoreni sadržaj, eng. *deep fakes*) te za manipuliranje takvim sadržajem, također bi trebali jasno istaknuti da je sadržaj umjetno stvoren ili da je njime manipulirano označivanjem izlaznih rezultata umjetne inteligencije i navođenjem njegova umjetnog podrijetla. Usklađenost s tom obvezom transparentnosti ne bi se trebala tumačiti niti kao da upućuje na to da se korištenjem UI sustava ili njegovih izlaznih rezultata ugrožava pravo na slobodu izražavanja i pravo na slobodu umjetnosti i znanosti koja su zajamčena Poveljom, posebno ako je sadržaj očito dio kreativnog, satiričkog, umjetničkog, fiktivnog ili analognog djela ili programa, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana. U tim je slučajevima obveza transparentnosti za uvjerljiv krivotvoreni sadržaj utvrđena u ovoj Uredbi ograničena na otkrivanje postojanja takvog generiranog ili manipuliranog sadržaja na odgovarajući način kojim se ne ometa prikazivanje djela ili uživanje u njemu, uključujući njegovo uobičajeno iskorištavanje i upotrebu, uz istodobno održavanje korisnosti i kvalitete djela. Osim toga, primjereno je predvidjeti sličnu obvezu otkrivanja u odnosu na tekst stvoren ili manipuliran umjetnom inteligencijom u mjeri u kojoj se objavljuje u svrhu informiranja javnosti o pitanjima od javnog interesa, osim ako je sadržaj stvoren umjetnom inteligencijom prošao proces preispitivanja koje provodi čovjek ili uredničku kontrolu i ako fizička ili pravna osoba snosi uredničku odgovornost za objavu sadržaja.

- (135) Ne dovodeći u pitanje obveznu prirodu i potpunu primjenjivost obveza u pogledu transparentnosti, Komisija može poticati i olakšavati izradu kodeksâ prakse na razini Unije kako bi se olakšala djelotvorna provedba obveza u pogledu otkrivanja i označivanja umjetno stvorenog ili manipuliranog sadržaja, među ostalim i kako bi se poduprla praktična rješenja za osiguravanje dostupnosti, prema potrebi, mehanizama za otkrivanje i olakšavanje suradnje s drugim akterima duž vrijednosnog lanca, širenje sadržaja ili provjera njegove autentičnosti i podrijetla kako bi se javnosti omogućilo djelotvorno prepoznavanje sadržaja stvorenog umjetnom inteligencijom.
- (136) Obveze propisane u ovoj Uredbi za dobavljače i za subjekte koji uvode određene UI sustave kako bi se omogućilo prepoznavanje i otkrivanje umjetno stvorenih ili manipuliranih izlaznih rezultata tih sustava posebno su relevantne za olakšavanje djelotvorne provedbe Uredbe (EU) 2022/2065. To se osobito odnosi na obveze pružatelja vrlo velikih internetskih platformi ili vrlo velikih internetskih tražilica da utvrde i ublaže sistemske rizike koji mogu proizaći iz širenja umjetno stvorenog ili manipuliranog sadržaja, posebno rizik od stvarnih ili predvidljivih negativnih učinaka na demokratske procese, građanski diskurs i izborne procese, među ostalim dezinformiranjem. Zahtjevom u pogledu označivanja sadržaja koji generiraju UI sustavi na temelju ove Uredbe ne dovodi se u pitanje obveza iz članka 16. stavka 6. Uredbe (EU) 2022/2065 prema kojoj pružatelji usluga smještaja informacija na poslužitelju moraju obrađivati prijave nezakonitog sadržaja zaprimljene na temelju članka 16. stavka 1. te uredbe i on ne bi trebao utjecati na procjenu i odluku o nezakonitosti određenog sadržaja. Ta bi se ocjena trebala provesti isključivo s obzirom na pravila kojima se uređuje zakonitost sadržaja.

- (137) Sukladnost s obvezama u pogledu transparentnosti za UI sustave obuhvaćene ovom Uredbom ne bi se trebala tumačiti kao da upućuje na to da je upotreba UI sustava ili njegovih izlaznih rezultata zakonita na temelju ove Uredbe ili drugog prava Unije i prava država članica i njome se ne bi trebale dovoditi u pitanje druge obveze u pogledu transparentnosti za subjekte koji uvode UI sustave koje su utvrđene u pravu Unije ili u nacionalnom pravu.
- (138) Umjetna inteligencija skup je tehnologija koje se vrlo brzo razvijaju, što zahtijeva regulatorni nadzor i siguran i kontroliran prostor za eksperimentiranje, pri čemu se osigurava da se inovacije razvijaju na odgovoran način te da se integriraju odgovarajuće zaštitne mjere i mjere za ublažavanje rizika. Kako bi se osigurao pravni okvir kojim se promiču inovacije te koji je spreman za buduće promjene i otporan na poremećaje, države članice trebale bi zajamčiti da njihova nacionalna nadležna tijela uspostave barem jedno regulatorno izolirano okruženje za umjetnu inteligenciju na nacionalnoj razini radi lakšeg razvoja i testiranja inovativnih UI sustava pod strogim regulatornim nadzorom prije stavljanja tih sustava na tržište ili u upotrebu. Države članice mogle bi ispuniti tu obvezu i sudjelovanjem u već postojećim regulatornim izoliranim okruženjima ili zajedničkom uspostavom izoliranog okruženja s jednim ili više nadležnih tijela država članica, u mjeri u kojoj se tim sudjelovanjem osigurava jednaka razina nacionalne pokrivenosti za države članice sudionice. Regulatorna izolirana okruženja za umjetnu inteligenciju mogla bi se uspostaviti u fizičkom, digitalnom ili hibridnom obliku te mogu uključivati fizičke i digitalne proizvode. Tijela nadležna za uspostavu regulatornih izoliranih okruženja za umjetnu inteligenciju trebala bi osigurati i da regulatorna izolirana okruženja imaju odgovarajuće resurse za njihovo funkcioniranje, uključujući financijske i ljudske resurse.

- (139) Ciljevi regulatornih izoliranih okruženja za umjetnu inteligenciju trebali bi biti poticanje inovacija u području umjetne inteligencije uspostavom kontroliranog okruženja za eksperimentiranje i testiranje u fazi razvoja i prije stavljanja na tržište kako bi se osigurala usklađenost inovativnih UI sustava s ovom Uredbom i drugim relevantnim pravom Unije i nacionalnim pravom. Nadalje, regulatornim izoliranim okruženjima za umjetnu inteligenciju trebalo bi nastojati povećati pravnu sigurnost za inovatore, poboljšati nadzor koji provode nadležna tijela i njihovo razumijevanje mogućnosti, novih rizika i učinaka upotrebe umjetne inteligencije, olakšati regulatorno učenje za nadležna tijela i poduzeća, među ostalim radi budućih prilagodbi pravnog okvira, poduprijeti suradnju i razmjenu primjera najbolje prakse s tijelima uključenima u regulatorno izolirano okruženje za umjetnu inteligenciju te ubrzati pristup tržištima, među ostalim uklanjanjem zapreka za MSP-ove, uključujući *start-up* poduzeća. Regulatorna izolirana okruženja za umjetnu inteligenciju trebala bi biti široko dostupna u cijeloj Uniji, a posebnu pozornost trebalo bi posvetiti njihovoj pristupačnosti za MSP-ove, uključujući *start-up* poduzeća. Sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju trebalo bi biti usmjereno na pitanja koja uzrokuju pravnu nesigurnost za dobavljače i potencijalne dobavljače u pogledu inovacija, eksperimentiranja s umjetnom inteligencijom u Uniji i doprinosa regulatornom učenju utemeljenom na dokazima. Nadzor UI sustava u regulatornom izoliranom okruženju za umjetnu inteligenciju stoga bi trebao obuhvaćati njihov razvoj, treniranje, testiranje i validaciju prije stavljanja tih sustava na tržište ili u upotrebu, kao i pojam i pojavu znatne izmjene koja bi mogla zahtijevati novi postupak ocjenjivanja sukladnosti. Ako se tijekom razvoja i testiranja takvih UI sustava uoče znatni rizici, ti bi se rizici trebali smanjiti na primjeren način, a ako to nije moguće, treba se prekinuti postupak razvoja i testiranja sve dok se oni ne smanje.

Nacionalna nadležna tijela koja uspostavljaju regulatorna izolirana okruženja za umjetnu inteligenciju trebala bi prema potrebi surađivati s drugim relevantnim tijelima, među ostalim s tijelima koja nadziru zaštitu temeljnih prava, i mogla bi omogućiti sudjelovanje drugih aktera iz ekosustava umjetne inteligencije, kao što su nacionalne ili europske organizacije za normizaciju, prijavljena tijela, objekti za testiranje i eksperimentiranje, laboratoriji za istraživanje i eksperimentiranje, europski centri za digitalne inovacije i relevantne organizacije dionika i organizacije civilnog društva. Radi ujednačene provedbe u cijeloj Uniji i ekonomije razmjera, primjereno je uspostaviti zajednička pravila za primjenu regulatornih izoliranih okruženja za umjetnu inteligenciju i okvir za suradnju relevantnih tijela uključenih u nadzor izoliranih okruženja. Regulatornim izoliranim okruženjima za umjetnu inteligenciju uspostavljenima na temelju ove Uredbe ne bi se trebalo dovoditi u pitanje drugo pravo kojim se omogućuje uspostava drugih izoliranih okruženja u cilju osiguravanja usklađenosti s pravom koje nije ova Uredba. Relevantna nadležna tijela zadužena za ta druga regulatorna izolirana okruženja trebala bi prema potrebi razmotriti prednosti upotrebe tih izoliranih okruženja i za potrebe osiguravanja usklađenosti UI sustavâ s ovom Uredbom. Slijedom dogovora između nacionalnih nadležnih tijela i sudionikâ u regulatornom izoliranom okruženju za umjetnu inteligenciju testiranje u stvarnim uvjetima može se također provoditi i nadzirati u okviru regulatornog izoliranog okruženja za umjetnu inteligenciju.

- (140) Ovom bi se Uredbom dobavljačima i potencijalnim dobavljačima u regulatornom izoliranom okruženju za umjetnu inteligenciju trebala osigurati pravna osnova za upotrebu osobnih podataka prikupljenih u druge svrhe za razvoj određenih UI sustava u javnom interesu u regulatornom izoliranom okruženju za umjetnu inteligenciju, samo pod određenim uvjetima, u skladu s člankom 6. stavkom 4. i člankom 9. stavkom 2. točkom (g) Uredbe (EU) 2016/679 i člancima 5., 6. i 10. Uredbe (EU) 2018/1725 te ne dovodeći u pitanje članak 4. stavak 2. i članak 10. Direktive (EU) 2016/680. I dalje se primjenjuju sve ostale obveze voditeljâ obrade podataka i prava ispitanikâ na temelju uredaba (EU) 2016/679 i (EU) 2018/1725 te Direktive (EU) 2016/680. Ovom Uredbom osobito se ne bi trebala osigurati pravna osnova u smislu članka 22. stavka 2. točke (b) Uredbe (EU) 2016/679 i članka 24. stavka 2. točke (b) Uredbe (EU) 2018/1725. Dobavljači i potencijalni dobavljači u regulatornom izoliranom okruženju za umjetnu inteligenciju trebali bi osigurati odgovarajuće zaštitne mjere i surađivati s nadležnim tijelima, među ostalim tako da slijede njihove smjernice i postupaju žurno i u dobroj vjeri kako bi se na primjeren način ublažili svi utvrđeni znatni rizici za sigurnost, zdravlje i temeljna prava koji mogu nastati tijekom razvoja, testiranja i eksperimentiranja u tom izoliranom okruženju.

- (141) Kako bi se ubrzao proces razvoja i stavljanja na tržište visokorizičnih UI sustava navedenih u prilogu ovoj Uredbi, važno je da se dobavljači ili potencijalni dobavljači takvih sustava mogu služiti posebnim režimom za testiranje tih sustava u stvarnim uvjetima, bez sudjelovanja u regulatornom izoliranom okruženju za umjetnu inteligenciju. Međutim, u takvim slučajevima, uzimajući u obzir moguće posljedice takvog testiranja na pojedince, trebalo bi osigurati da se ovom Uredbom uvedu odgovarajuća i dostatna jamstva i uvjeti za dobavljače ili potencijalne dobavljače. Takva bi jamstva među ostalim trebala uključivati traženje informiranog pristanka fizičke osobe za sudjelovanje u testiranju u stvarnim uvjetima, uz iznimku tijela kaznenog progona ako bi traženje informiranog pristanka spriječilo testiranje UI sustava. Pristanak ispitanika za sudjelovanje u takvom testiranju na temelju ove Uredbe razlikuje se od privole ispitanika za obradu njihovih osobnih podataka na temelju relevantnog zakonodavstva o zaštiti podataka i njime se privola za obradu osobnih podataka ne dovodi u pitanje.

Također je važno smanjiti rizike i omogućiti nadzor od strane nadležnih tijela te stoga zahtijevati od potencijalnih dobavljača da imaju plan testiranja u stvarnim uvjetima koji se podnosi nadležnom tijelu za nadzor tržišta, da registriraju testiranje u posebnim odjeljcima u bazi podataka EU-a podložno određenim ograničenim iznimkama, da utvrde ograničenja u pogledu razdoblja u kojem se testiranje može provesti i da zahtijevaju dodatne zaštitne mjere za osobe koje pripadaju određenim skupinama ranjivih osoba, kao i pisani sporazum kojim se utvrđuju uloge i odgovornosti potencijalnih dobavljača i subjekata koji uvode sustav te djelotvoran nadzor koji provodi nadležno osoblje uključeno u testiranje u stvarnim uvjetima. Nadalje, primjereno je predvidjeti dodatne zaštitne mjere kako bi se osiguralo da se predviđanja, preporuke ili odluke UI sustava mogu djelotvorno poništiti i zanemariti te da se osobni podaci zaštite i brišu ako ispitanici povuku svoj pristanak za sudjelovanje u testiranju, ne dovodeći u pitanje prava koja imaju kao ispitanici u skladu s pravom Unije o zaštiti podataka. Kad je riječ o prijenosu podataka, također je primjereno predvidjeti da bi se podaci prikupljeni i obrađeni u svrhu testiranja u stvarnim uvjetima trebali prenositi trećim zemljama samo ako se provode odgovarajuće i primjenjive zaštitne mjere na temelju prava Unije, posebno u skladu s osnovama za prijenos osobnih podataka na temelju prava Unije o zaštiti podataka, dok su za neosobne podatke uspostavljene odgovarajuće zaštitne mjere u skladu s pravom Unije, kao što su uredbe (EU) 2022/868⁴² i (EU) 2023/2854⁴³ Europskog parlamenta i Vijeća.

⁴² Uredba (EU) 2022/868 Europskog parlamenta i Vijeća od 30. svibnja 2022. o europskom upravljanju podacima i izmjeni Uredbe (EU) 2018/1724 (Akt o upravljanju podacima) (SL L 152, 3.6.2022., str. 1.).

⁴³ Uredba (EU) 2023/2854 Europskog parlamenta i Vijeća od 13. prosinca 2023. o usklađenim pravilima za pravedan pristup podacima i njihovu uporabu i o izmjeni Uredbe (EU) 2017/2394 i Direktive (EU) 2020/1828 (Akt o podacima) (SL L, 2023/2854, 22.12.2023., ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

- (142) Kako bi se osiguralo da umjetna inteligencija dovede do društveno i okolišno korisnih ishoda, države članice potiču se da podupiru i promiču istraživanje i razvoj UI rješenja kojima se podupiru ishodi korisni za društvo i okoliš, kao što su rješenja koja se temelje na umjetnoj inteligenciji za povećanje pristupačnosti za osobe s invaliditetom, uklanjanje socioekonomskih nejednakosti ili postizanje okolišnih ciljeva dodjelom dostatnih sredstava, uključujući javno financiranje i financiranje sredstvima Unije, te, prema potrebi i pod uvjetom da su ispunjeni kriteriji prihvatljivosti i odabira, posebno uzimajući u obzir projekte kojima se nastoje ostvariti takvi ciljevi. Takvi bi se projekti trebali temeljiti na načelu interdisciplinarne suradnje među razvojnim programerima umjetne inteligencije, stručnjacima za nejednakost i nediskriminaciju, pristupačnost te potrošačka, okolišna i digitalna prava te akademskom zajednicom.

- (143) Kako bi se promicale i štitile inovacije, posebno je važno uzeti u obzir interese MSP-ova, među ostalima i *start-up* poduzeća, koji su dobavljači UI sustava ili subjekti koji ih uvode. U tom cilju bi države članice trebale osmisliti inicijative usmjerene na te operatere, među ostalim u pogledu podizanja svijesti i informiranja. Države članice trebale bi MSP-ovima, među ostalim i *start-up* poduzećima, koji imaju registrirano sjedište ili podružnicu u Uniji, osiguravati prioritetni pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju, pod uvjetom da ispunjavaju uvjete prihvatljivosti i kriterije za odabir te da drugim dobavljačima i potencijalnim dobavljačima ne onemogućuju pristup izoliranim okruženjima pod uvjetom da su ispunjeni isti uvjeti i kriteriji. Države članice trebale bi se koristiti postojećim kanalima i, prema potrebi, uspostaviti nove namjenske kanale za komunikaciju s MSP-ovima, među ostalim i *start-up* poduzećima, subjektima koji uvode sustav, drugim inovatorima i, prema potrebi, lokalnim tijelima javne vlasti, radi podupiranja MSP-ova tijekom cijelog njihova razvoja pružanjem smjernica i odgovaranjem na upite o provedbi ove Uredbe. Prema potrebi, ti kanali trebali bi međusobno surađivati kako bi se stvorila sinergija i osigurala homogenost smjernica za MSP-ove, uključujući *start-up* poduzeća, i subjekte koji uvode sustav. Osim toga, države članice trebale bi olakšavati sudjelovanje MSP-ova i drugih relevantnih dionika u procesima razvoja normizacije. Usto, prijavljena tijela trebala bi uzeti u obzir posebne interese i potrebe dobavljača koji su MSP-ova, među ostalima i onih koji su *start-up* poduzeća, kad određuju naknade za ocjenjivanje sukladnosti. Komisija bi s pomoću transparentnog savjetovanja trebala redovito ocjenjivati troškove certifikacije i usklađivanja za MSP-ove, među ostalima i za *start-up* poduzeća, te surađivati s državama članicama u cilju smanjenja takvih troškova.

Na primjer, dobavljači i drugi operateri, posebno oni manji, mogu imati znatne troškove prijevoda obvezne dokumentacije i komunikacije s tijelima. Države članice trebale bi možda osigurati da jedan od jezika koji odrede i prihvaćaju za relevantnu dokumentaciju dobavljača i komunikaciju s operaterima bude jedan od jezika koji u velikoj mjeri razumije najveći mogući broj prekograničnih subjekata koji uvode sustav. Kako bi se odgovorilo na posebne potrebe MSP-ova, uključujući *start-up* poduzeća, Komisija bi na zahtjev Vijeća za umjetnu inteligenciju trebala osigurati standardizirane predloške za područja obuhvaćena ovom Uredbom. Osim toga, Komisija bi trebala dopuniti napore država članica osiguravanjem jedinstvene informacijske platforme koja pruža informacije o ovoj Uredbi jednostavne za upotrebu za sve dobavljače i subjekte koji uvode sustav, organiziranjem odgovarajućih komunikacijskih kampanja za podizanje svijesti o obvezama koje proizlaze iz ove Uredbe te evaluacijom i promicanjem konvergencije primjera najbolje prakse u postupcima javne nabave u vezi s UI sustavima. Srednja poduzeća koja su do nedavno ispunjavala uvjete za mala poduzeća u smislu Priloga Preporuci Komisije 2003/361/EZ⁴⁴ trebala bi imati pristup tim mjerama potpore jer tim novim srednjim poduzećima ponekad možda nedostaju pravni resursi i osposobljavanje potrebni za osiguravanje pravilnog razumijevanja i usklađenosti s ovom Uredbom.

⁴⁴ Preporuka Komisije od 6. svibnja 2003. o definiciji mikro, malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

- (144) Kako bi se promicale i zaštitile inovacije, ostvarivanju ciljeva ove Uredbe trebalo bi, prema potrebi, doprinosti putem platforme za umjetnu inteligenciju na zahtjev i svih relevantnih programa i projekata za financiranje sredstvima Unije, poput programa Digitalna Europa i Obzor Europa, koje provode Komisija i države članice na razini Unije ili nacionalnoj razini.
- (145) Kako bi se rizici za provedbu koji proizlaze iz nedostatka znanja i iskustva na tržištu sveli na najmanju moguću mjeru i kako bi se dobavljačima, posebno MSP-ovima, uključujući *start-up* poduzeća, i prijavljenim tijelima olakšalo ispunjavanje obveza iz ove Uredbe, provedbi ove Uredbe trebalo bi doprinosti putem platforme za umjetnu inteligenciju na zahtjev, europskih centara za digitalne inovacije te centara za testiranje i eksperimentiranje koje uspostavljaju Komisija i države članice na razini Unije ili nacionalnoj razini. U okviru svoje misije i područja nadležnosti, platforma za umjetnu inteligenciju na zahtjev, europski centri za digitalne inovacije te centri za testiranje i eksperimentiranje mogu posebno pružati tehničku i znanstvenu potporu dobavljačima i prijavljenim tijelima.

- (146) Nadalje, s obzirom na vrlo malenu veličinu pojedinih operatera i kako bi se osigurala proporcionalnost u pogledu troškova inovacija, primjereno je omogućiti mikropoduzećima da ispune jednu od najskupljih obveza, a to je uspostava sustava upravljanja kvalitetom, na pojednostavnjen način, čime bi se smanjili administrativno opterećenje i troškovi za ta poduzeća, a bez utjecaja na razinu zaštite i potrebu za usklađivanjem sa zahtjevima za visokorizične UI sustave. Komisija bi trebala izraditi smjernice za određivanje elemenata sustava upravljanja kvalitetom koje mikropoduzeća moraju ispuniti na taj pojednostavnjen način.
- (147) Primjereno je da Komisija olakša, u mjeri u kojoj je to moguće, pristup centrima za testiranje i eksperimentiranje tijelima, skupinama ili laboratorijima uspostavljenima ili akreditiranim na temelju bilo kojeg dijela zakonodavstva Unije o usklađivanju, a koji obavljaju zadaće u kontekstu postupaka ocjenjivanja sukladnosti proizvoda ili uređaja obuhvaćenih tim zakonodavstvom Unije o usklađivanju. To se posebno odnosi na stručne skupine, stručne laboratorije i referentne laboratorije u području medicinskih proizvoda na temelju uredaba (EU) 2017/745 i (EU) 2017/746.

(148) Ovom bi se Uredbom trebao uspostaviti okvir upravljanja koji omogućuje i koordinaciju primjene ove Uredbe na nacionalnoj razini i potporu primjeni ove Uredbe na nacionalnoj razini, kao i izgradnju kapaciteta na razini Unije i integraciju dionika u području umjetne inteligencije. Za djelotvornu provedbu i izvršavanje ove Uredbe potreban je okvir upravljanja koji omogućuje koordinaciju i prikupljanje središnjeg stručnog znanja na razini Unije. Ured za umjetnu inteligenciju osnovan je Odlukom Komisije⁴⁵, a njegova je zadaća razvoj stručnog znanja i sposobnosti Unije u području umjetne inteligencije te doprinos provedbi prava Unije o umjetnoj inteligenciji. Države članice trebale bi olakšati zadaće Ureda za umjetnu inteligenciju kako bi se podržao razvoj stručnog znanja i sposobnosti Unije na razini Unije te ojačalo funkcioniranje jedinstvenog digitalnog tržišta. Nadalje, trebalo bi osnovati Vijeće za umjetnu inteligenciju koje se sastoji od predstavnika država članica, znanstveno povjerenstvo za integraciju znanstvene zajednice i savjetodavni forum za doprinos dionika provedbi ove Uredbe, na razini Unije i na nacionalnoj razini. Razvoj stručnog znanja i sposobnosti Unije trebao bi uključivati i iskorištavanje postojećih resursa i stručnog znanja, posebno putem sinergije sa strukturama uspostavljenima u kontekstu provedbe drugog prava i sinergije s povezanim inicijativama na razini Unije, kao što su Zajedničko poduzeće EuroHPC i objekti za testiranje i eksperimentiranje umjetne inteligencije u okviru programa Digitalna Europa.

⁴⁵ Odluka Komisije od 24. siječnja 2024. o osnivanju Europskog ureda za umjetnu inteligenciju C(2024) 390.

- (149) Kako bi se olakšala nesmetana, djelotvorna i usklađena provedba ove Uredbe, trebalo bi osnovati Vijeće za umjetnu inteligenciju. U Vijeću za umjetnu inteligenciju trebali bi se odražavati različiti interesi ekosustava umjetne inteligencije, a trebao bi biti sastavljen od predstavnika država članica. Vijeće za umjetnu inteligenciju trebalo bi biti odgovorno za niz savjetodavnih zadaća, uključujući davanje mišljenja, preporuka i savjeta ili doprinošenje smjernicama o pitanjima povezanim s provedbom ove Uredbe, među ostalim pitanjima izvršenja, tehničkim specifikacijama ili postojećim normama povezanim sa zahtjevima ove Uredbe, te za davanje savjeta Komisiji i državama članicama te njihovim nacionalnim nadležnim tijelima u vezi sa specifičnim pitanjima povezanim s umjetnom inteligencijom. Kako bi se državama članicama pružila određena fleksibilnost u vezi s imenovanjem njihovih predstavnika u Vijeće za umjetnu inteligenciju, ti predstavnici mogu biti sve osobe koje pripadaju javnim subjektima i koje bi trebale imati odgovarajuće nadležnosti i ovlasti za olakšavanje koordinacije na nacionalnoj razini i doprinošenje ostvarivanju zadaća Vijeća za umjetnu inteligenciju. Vijeće za umjetnu inteligenciju trebalo bi osnovati dvije stalne podskupine kako bi osigurao platformu za suradnju i razmjenu između tijela za nadzor tržišta i tijela koja provode prijavljivanje o pitanjima koja se odnose na nadzor tržišta odnosno na prijavljena tijela. Stalna podskupina za nadzor tržišta trebala bi djelovati kao skupina za administrativnu suradnju (ADCO) za ovu Uredbu u smislu članka 30. Uredbe (EU) 2019/1020. U skladu s člankom 33. te uredbe Komisija bi trebala podupirati aktivnosti stalne podskupine za nadzor tržišta provođenjem evaluacija ili studija tržišta, osobito u cilju utvrđivanja aspekata ove Uredbe koji zahtijevaju posebnu i hitnu koordinaciju među tijelima za nadzor tržišta. Vijeće za umjetnu inteligenciju prema potrebi može osnovati druge stalne ili privremene podskupine za razmatranje specifičnih pitanja. Vijeće za umjetnu inteligenciju također bi prema potrebi trebalo surađivati s relevantnim tijelima Unije, stručnim skupinama i mrežama koje djeluju u kontekstu relevantnog prava Unije, uključujući posebno one koje djeluju na temelju relevantnog prava Unije o podacima, digitalnim proizvodima i uslugama.

- (150) Kako bi se osiguralo sudjelovanje dionika u provedbi i primjeni ove Uredbe, trebalo bi uspostaviti savjetodavni forum radi savjetovanja Vijeća za umjetnu inteligenciju i Komisije i pružanja tehničkog stručnog znanja Vijeću za umjetnu inteligenciju i Komisiji. Kako bi se osigurala raznolika i uravnotežena zastupljenost dionika s komercijalnim i nekomercijalnim interesima te, unutar kategorije komercijalnih interesa, u pogledu MSP-ova i drugih poduzeća, savjetodavni forum trebao bi obuhvaćati, među ostalim, industriju, *start-up* poduzeća, MSP-ove, akademsku zajednicu, civilno društvo, uključujući socijalne partnere, kao i Agenciju za temeljna prava, ENISA-u, Europski odbor za normizaciju (CEN), Europski odbor za elektrotehničku normizaciju (CENELEC) i Europski institut za telekomunikacijske norme (ETSI).
- (151) Kako bi se poduprli provedba i izvršavanje ove Uredbe, osobito aktivnosti praćenja koje provodi Ured za umjetnu inteligenciju u pogledu UI modelâ opće namjene, trebalo bi osnovati znanstveno povjerenstvo neovisnih stručnjaka. Neovisni stručnjaci koji čine znanstveno povjerenstvo trebali bi se birati na temelju najnovijeg znanstvenog ili tehničkog stručnog znanja u području umjetne inteligencije te bi trebali obavljati svoje zadaće nepristrano i objektivno te osigurati povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti. Kako bi se omogućilo jačanje nacionalnih kapaciteta potrebnih za djelotvorno izvršavanje ove Uredbe, države članice trebale bi za svoje aktivnosti izvršavanja moći zatražiti potporu skupine stručnjaka koji čine znanstveno povjerenstvo.

- (152) Kako bi se poduprlo odgovarajuće izvršavanje u vezi s UI sustavima i ojačali kapaciteti država članica, trebalo bi uspostaviti potporne strukture Unije za testiranje umjetne inteligencije i staviti ih na raspolaganje državama članicama.
- (153) Države članice imaju ključnu ulogu u primjeni i izvršavanju ove Uredbe. Svaka bi država članica stoga trebala imenovati barem jedno tijelo koje provodi prijavljivanje i barem jedno tijelo za nadzor tržišta kao nacionalna nadležna tijela za potrebe nadziranja primjene i provedbe ove Uredbe. Države članice mogu odlučiti imenovati bilo koju vrstu javnog subjekta za obavljanje zadaća nacionalnih nadležnih tijela u smislu ove Uredbe, u skladu sa svojim posebnim nacionalnim organizacijskim karakteristikama i potrebama. Kako bi se povećala učinkovitost organizacije u državama članicama i uspostavila jedinstvena kontaktna točka za javne i druge partnere na razini država članica i na razini Unije, svaka bi država članica trebala imenovati tijelo za nadzor tržišta koje će djelovati kao jedinstvena kontaktna točka.
- (154) Ta nacionalna nadležna tijela trebala bi izvršavati svoje ovlasti neovisno, objektivno i nepristrano kako bi zaštitila načela objektivnosti svojih aktivnosti i zadaća te osigurala primjenu i provedbu ove Uredbe. Članovi tih tijela trebali bi se suzdržati od svakog djelovanja koje nije u skladu s njihovim dužnostima te bi trebali podlijegati pravilima o povjerljivosti na temelju ove Uredbe.

- (155) Kako bi se osiguralo da dobavljači visokorizičnih UI sustava mogu uzeti u obzir iskustvo stečeno korištenjem visokorizičnih UI sustava za poboljšanje svojih sustava te za proces dizajniranja i razvoja ili da mogu pravodobno poduzeti korektivne mjere, svi bi dobavljači trebali uspostaviti sustav praćenja nakon stavljanja na tržište. Ako je to relevantno, praćenje nakon stavljanja na tržište trebalo bi obuhvaćati analizu interakcije s drugim UI sustavima, uključujući druge uređaje i softver. Praćenje nakon stavljanja na tržište ne bi trebalo obuhvaćati osjetljive operativne podatke subjekata koji uvode sustav koji su tijela kaznenog progona. Taj je sustav ključan i za učinkovitije i pravodobnije poduzimanje mjera povezanih s mogućim rizicima od UI sustava koji „uče” i nakon što su stavljeni na tržište ili u upotrebu. U tom bi kontekstu od dobavljača trebalo također zahtijevati da uspostave sustav za prijavljivanje relevantnim tijelima svih ozbiljnih incidenata koji su posljedica korištenja njihovih UI sustava, odnosno incidenta ili neispravnosti koji dovode do smrti ili teške štete za zdravlje, ozbiljnih i nepovratnih poremećaja u upravljanju kritičnom infrastrukturom i njezinu radu, povreda obveza na temelju prava Unije namijenjenih zaštititi temeljnih prava ili teške štete za imovinu ili okoliš.

- (156) Kako bi se osiguralo odgovarajuće i djelotvorno izvršavanje zahtjeva i obveza utvrđenih u ovoj Uredbi, koja je zakonodavstvo Unije o usklađivanju, u cijelosti bi se trebao primjenjivati sustav nadzora tržišta i sukladnosti proizvoda uspostavljen Uredbom (EU) 2019/1020. Tijela za nadzor tržišta imenovana na temelju ove Uredbe trebala bi imati sve ovlasti izvršavanja utvrđene u ovoj Uredbi i u Uredbi (EU) 2019/1020 i svoje bi ovlasti i dužnosti trebala izvršavati neovisno, objektivno i nepristrano. Iako većina UI sustava ne podliježe posebnim zahtjevima i obvezama na temelju ove Uredbe, tijela za nadzor tržišta mogu poduzeti mjere u vezi sa svim UI sustavima kada oni predstavljaju rizik u skladu s ovom Uredbom. Zbog specifične prirode institucija, agencija i tijela Unije obuhvaćenih područjem primjene ove Uredbe primjereno je za njih imenovati Europskog nadzornika za zaštitu podataka tijelom nadležnim za nadzor tržišta. Time se ne bi trebalo dovoditi u pitanje imenovanje nacionalnih nadležnih tijela koje provode države članice. Aktivnosti nadzora tržišta ne bi trebale utjecati na sposobnost nadziranih subjekata da neovisno obavljaju svoje zadaće kada se takva neovisnost zahtijeva pravom Unije.

- (157) Ovom se Uredbom ne dovode u pitanje nadležnosti, zadaće, ovlasti i neovisnost relevantnih nacionalnih tijela javne vlasti ili javnih tijela koja nadziru primjenu prava Unije o zaštiti temeljnih prava, uključujući tijela za ravnopravnost i tijela za zaštitu podataka. Ako je to potrebno za njihov mandat, ta nacionalna tijela javne vlasti ili javna tijela trebala bi također imati pristup svojoj dokumentaciji izrađenoj na temelju ove Uredbe. Trebalo bi utvrditi poseban zaštitni postupak kako bi se osiguralo adekvatno i pravodobno izvršavanje u pogledu UI sustava koji predstavljaju rizik za zdravlje, sigurnost i temeljna prava. Postupak za takve UI sustave koji predstavljaju rizik trebao bi se primjenjivati na visokorizične UI sustave koji predstavljaju rizik, zabranjene sustave koji su stavljeni na tržište, stavljeni u upotrebu ili se upotrebljavaju protivno odredbama o zabranjenim praksama iz ove Uredbe i na UI sustave koji su stavljeni na raspolaganje protivno odredbama o zahtjevima u pogledu transparentnosti iz ove Uredbe i koji predstavljaju rizik.

- (158) Pravo Unije o financijskim uslugama uključuje pravila i zahtjeve o unutarnjem upravljanju i upravljanju rizikom koji se primjenjuju na regulirane financijske institucije pri pružanju tih usluga, među ostalim kad upotrebljavaju UI sustave. Kako bi se osigurala dosljedna primjena i izvršavanje obveza iz ove Uredbe te relevantnih pravila i zahtjeva iz pravnih akata Unije o financijskim uslugama, nadležna tijela odgovorna za nadzor i izvršavanje tih pravnih akata, posebno nadležna tijela kako su definirana u Uredbi (EU) br. 575/2013 Europskog parlamenta i Vijeća⁴⁶ i direktivama 2008/48/EZ⁴⁷, 2009/138/EZ⁴⁸, 2013/36/EU⁴⁹, 2014/17/EU⁵⁰ i (EU) 2016/97⁵¹ Europskog parlamenta i Vijeća, trebala bi biti imenovana, u okviru vlastitih nadležnosti, nadležnim tijelima za potrebe nadziranja provedbe ove Uredbe, među ostalim i za aktivnosti nadzora tržišta, kad je riječ o UI sustavima koje pružaju ili upotrebljavaju financijske institucije koje su regulirane i pod nadzorom, osim ako države članice odluče za obavljanje tih zadaća nadzora tržišta imenovati drugo tijelo.

⁴⁶ Uredba (EU) br. 575/2013 Europskog parlamenta i Vijeća od 26. lipnja 2013. o bonitetnim zahtjevima za kreditne institucije i investicijska društva i o izmjeni Uredbe (EU) br. 648/2012 (SL L 176, 27.6.2013., str. 1.).

⁴⁷ Direktiva 2008/48/EZ Europskog parlamenta i Vijeća od 23. travnja 2008. o ugovorima o potrošačkim kreditima i stavljanju izvan snage Direktive Vijeća 87/102/EEZ (SL L 133, 22.5.2008., str. 66.).

⁴⁸ Direktiva 2009/138/EZ Europskog parlamenta i Vijeća od 25. studenoga 2009. o osnivanju i obavljanju djelatnosti osiguranja i reosiguranja (Solventnost II) (SL L 335, 17.12.2009., str. 1.).

⁴⁹ Direktiva 2013/36/EU Europskog parlamenta i Vijeća od 26. lipnja 2013. o pristupanju djelatnosti kreditnih institucija i bonitetnom nadzoru nad kreditnim institucijama i investicijskim društvima, izmjeni Direktive 2002/87/EZ te stavljanju izvan snage direktiva 2006/48/EZ i 2006/49/EZ (SL L 176, 27.6.2013., str. 338.).

⁵⁰ Direktiva 2014/17/EU Europskog parlamenta i Vijeća od 4. veljače 2014. o ugovorima o potrošačkim kreditima koji se odnose na stambene nekretnine i o izmjeni direktiva 2008/48/EZ i 2013/36/EU i Uredbe (EU) br. 1093/2010 (SL L 60, 28.2.2014., str. 34.).

⁵¹ Direktiva (EU) 2016/97 Europskog parlamenta i Vijeća od 20. siječnja 2016. o distribuciji osiguranja (SL L 26, 2.2.2016., str. 19.).

Ta bi nadležna tijela trebala imati sve ovlasti na temelju ove Uredbe i Uredbe (EU) 2019/1020 za izvršavanje zahtjeva i obveza iz ove Uredbe, uključujući ovlasti za provođenje *ex post* aktivnosti nadzora tržišta koje se prema potrebi mogu integrirati u njihove postojeće nadzorne mehanizme i postupke na temelju relevantnog prava Unije o financijskim uslugama. Primjereno je predvidjeti da bi, kada djeluju kao tijela za nadzor tržišta na temelju ove Uredbe, nacionalna tijela odgovorna za nadziranje kreditnih institucija reguliranih Direktivom 2013/36/EU, koja sudjeluju u jedinstvenom nadzornom mehanizmu uspostavljenom Uredbom Vijeća (EU) br. 1024/2013⁵², trebala bez odgode izvijestiti Europsku središnju banku o svim informacijama utvrđenima tijekom njihovih aktivnosti nadzora tržišta koje bi mogle biti od interesa za zadaće bonitetnog nadzora Europske središnje banke navedene u toj uredbi. Kako bi se dodatno poboljšala usklađenost između ove Uredbe i pravila koja se primjenjuju na kreditne institucije regulirane Direktivom 2013/36/EU, također je primjereno integrirati neke od postupovnih obveza dobavljača povezanih s upravljanjem rizikom, praćenjem nakon stavljanja na tržište i vođenjem dokumentacije u postojeće obveze i postupke na temelju Direktive 2013/36/EU. Kako bi se izbjegla preklapanja, trebalo bi predvidjeti i ograničena odstupanja u pogledu sustava dobavljača za upravljanje kvalitetom i obveze praćenja za subjekte koji uvode visokorizične UI sustave u mjeri u kojoj se primjenjuju na kreditne institucije regulirane Direktivom 2013/36/EU. Isti bi se režim trebao primjenjivati na društva za osiguranje i reosiguranje i osigurateljne holdinge na temelju Direktive 2009/138/EZ i posrednike u osiguranju na temelju Direktive (EU) 2016/97 te na druge vrste financijskih institucija koje podliježu zahtjevima u pogledu unutarnjeg upravljanja, aranžmana ili postupaka uspostavljenih na temelju relevantnog prava Unije o financijskim uslugama kako bi se osigurala dosljednost i jednako postupanje u financijskom sektoru.

⁵² Uredba Vijeća (EU) br. 1024/2013 od 15. listopada 2013. o dodjeli određenih zadaća Europskoj središnjoj banci u vezi s politikama bonitetnog nadzora kreditnih institucija (SL L 287, 29.10.2013., str. 63.).

- (159) Svako tijelo za nadzor tržišta za visokorizične UI sustave u području biometrije, kako je navedeno u prilogu ovoj Uredbi, u mjeri u kojoj se ti sustavi upotrebljavaju u svrhu kaznenog progona, migracija, azila i upravljanja nadzorom državne granice ili za sudovanje i demokratske procese, trebalo bi imati djelotvorne istražne i korektivne ovlasti, uključujući barem ovlast za dobivanje pristupa svim osobnim podacima koji se obrađuju i svim informacijama potrebnima za obavljanje svojih zadaća. Tijela za nadzor tržišta trebala bi moći izvršavati svoje ovlasti potpuno neovisno. Bilo kakvim ograničenjima njihova pristupa osjetljivim operativnim podacima na temelju ove Uredbe ne bi se trebale dovoditi u pitanje ovlasti koje su im dodijeljene Direktivom (EU) 2016/680. Nijedno isključenje otkrivanja podataka nacionalnim tijelima za zaštitu podataka na temelju ove Uredbe ne bi trebalo utjecati na aktualne ili buduće ovlasti tih tijela izvan područja primjene ove Uredbe.
- (160) Tijela za nadzor tržišta i Komisija trebali bi moći predložiti zajedničke aktivnosti, uključujući zajedničke istrage, koje trebaju provoditi tijela za nadzor tržišta ili tijela za nadzor tržišta zajedno s Komisijom, a čiji je cilj promicanje sukladnosti, utvrđivanje nesukladnosti, podizanje svijesti i pružanje smjernica u vezi s ovom Uredbom u pogledu specifičnih kategorija visokorizičnih UI sustava za koje je utvrđeno da predstavljaju ozbiljan rizik u dvjema ili više država članica. Zajedničke aktivnosti u cilju promicanja sukladnosti trebale bi se provoditi u skladu s člankom 9. Uredbe (EU) 2019/1020. Ured za umjetnu inteligenciju trebao bi pružati koordinacijsku potporu za zajedničke istrage.

- (161) Potrebno je pojasniti odgovornosti i nadležnosti na razini Unije i na nacionalnoj razini u pogledu UI sustava koji se temelje na UI modelima opće namjene. Kako bi se izbjeglo preklapanje nadležnosti, ako se UI sustav temelji na UI modelu opće namjene, a model i sustav osigurava isti dobavljač, nadzor bi se trebao provoditi na razini Unije putem Ureda za umjetnu inteligenciju, koji bi u tu svrhu trebao imati ovlasti tijela za nadzor tržišta u smislu Uredbe (EU) 2019/1020. U svim ostalim slučajevima nacionalna tijela za nadzor tržišta i dalje su odgovorna za nadzor UI sustavâ. Međutim, kad je riječ o UI sustavima opće namjene koje subjekti koji uvode UI sustav mogu izravno upotrebljavati u barem jednu svrhu koja je klasificirana kao visokorizična, tijela za nadzor tržišta trebala bi surađivati s Uredom za umjetnu inteligenciju na provedbi evaluacija usklađenosti te o tome obavijestiti Vijeće za umjetnu inteligenciju i druga tijela za nadzor tržišta. Nadalje, tijela za nadzor tržišta trebala bi moći zatražiti pomoć od Ureda za umjetnu inteligenciju ako tijelo za nadzor tržišta ne može zaključiti istragu visokorizičnog UI sustava zbog toga što ne može pristupiti određenim informacijama povezanim s UI modelom opće namjene na kojem je izgrađen visokorizični UI sustav. U takvim bi se slučajevima postupak u pogledu uzajamne pomoći u prekograničnim slučajevima iz poglavlja VI. Uredbe (EU) 2019/1020 trebao primjenjivati *mutatis mutandis*.

- (162) Kako bi se na razini Unije na najbolji način iskoristilo centralizirano stručno znanje i sinergija Unije, ovlasti nadzora i izvršavanja obveza dobavljača UI modela opće namjene trebale bi biti u nadležnosti Komisije.. Ured za umjetnu inteligenciju trebao bi moći provoditi sve potrebne mjere za praćenje djelotvorne provedbe ove Uredbe u pogledu UI modela opće namjene. Trebao bi moći istražiti moguće povrede pravila o dobavljačima UI modela opće namjene na vlastitu inicijativu, na temelju rezultata svojih aktivnosti praćenja ili na zahtjev tijela za nadzor tržišta u skladu s uvjetima utvrđenima u ovoj Uredbi. Kako bi se poduprlo djelotvorno praćenje koje provodi Ured za umjetnu inteligenciju, trebalo bi predvidjeti mogućnost da dobavljači niže u lancu podnose pritužbe o mogućim povredama pravila o dobavljačima UI modela i sustava opće namjene.
- (163) Kako bi se dopunili sustavi upravljanja za UI modele opće namjene, znanstveno povjerenstvo trebalo bi podupirati aktivnosti praćenja koje provodi Ured za umjetnu inteligenciju i može, u određenim slučajevima, Uredu za umjetnu inteligenciju dostaviti kvalificirana upozorenja kojima se pokreću daljnje mjere, kao što su istrage. To bi trebao biti slučaj kada znanstveno povjerenstvo ima razloga sumnjati da UI model opće namjene predstavlja konkretan i utvrdiv rizik na razini Unije. Nadalje, to bi trebao biti slučaj kada znanstveno povjerenstvo ima razloga sumnjati da UI model opće namjene ispunjava kriterije koji bi doveli do toga da ga se klasificira kao UI model opće namjene sa sistemskim rizikom. Kako bi znanstveno povjerenstvo dobilo informacije potrebne za obavljanje tih zadaća, trebao bi postojati mehanizam kojim ono može zatražiti od Komisije da od dobavljača zatraži dokumentaciju ili informacije.

- (164) Ured za umjetnu inteligenciju trebao bi moći poduzeti potrebne mjere za praćenje djelotvorne provedbe i ispunjavanja obveza dobavljača UI modelâ opće namjene koje su utvrđene u ovoj Uredbi. Ured za umjetnu inteligenciju trebao bi moći istražiti moguće povrede u skladu s ovlastima predviđenima u ovoj Uredbi, među ostalim traženjem dokumentacije i informacija, provođenjem evaluacija i zahtijevanjem od dobavljača UI modela opće namjene da provede mjere. Kako bi se iskoristilo neovisno stručno znanje, pri provedbi evaluacija Ured za umjetnu inteligenciju trebao bi moći uključiti neovisne stručnjake da provedu evaluacije u njegovo ime. Usklađenost s obvezama trebala bi biti izvršiva, među ostalim, s pomoću zahtjevâ za poduzimanje odgovarajućih mjera, među ostalim i mjera za ublažavanje rizika u slučaju utvrđenih sistemskih rizika, kao i ograničavanja stavljanja na raspolaganje na tržištu, povlačenja ili opoziva modela. Kao zaštitna mjera, ako je to potrebno izvan okvira postupovnih prava predviđenih u ovoj Uredbi, dobavljači UI modela opće namjene trebali bi imati postupovna prava predviđena u članku 18. Uredbe (EU) 2019/1020, koji bi se trebao primjenjivati *mutatis mutandis*, ne dovodeći u pitanje specifičnija postupovna prava predviđena ovom Uredbom.

- (165) Razvoj UI sustava koji nisu visokorizični u skladu sa zahtjevima ove Uredbe može dovesti do šire primjene etične i pouzdane umjetne inteligencije u Uniji. Dobavljače UI sustava koji nisu visokorizični trebalo bi poticati na izradu kodeksâ ponašanja, uključujući povezane mehanizme upravljanja, namijenjenih poticanju dobrovoljne primjene nekih ili svih obveznih zahtjeva koji se primjenjuju na visokorizične UI sustave, prilagođenih namjeni sustava i manjem riziku te uzimajući u obzir dostupna tehnička rješenja i najbolje industrijske prakse kao što su kartice modela i podatkovne kartice. Dobavljače i, prema potrebi, subjekte koji uvode sve UI sustave, bez obzira na to jesu li visokorizični, i UI modele trebalo bi također poticati da dobrovoljno primjenjuju dodatne zahtjeve koji se odnose, na primjer, na elemente Etičkih smjernica Unije za pouzdanu umjetnu inteligenciju, okolišnu održivost, mjere pismenosti u području umjetne inteligencije, uključiv i raznolik dizajn i razvoj UI sustava, uključujući usmjeravanje pozornosti na ranjive osobe i pristupačnost za osobe s invaliditetom, sudjelovanje dionika uz uključenost, prema potrebi, relevantnih dionika kao što su poduzeća i organizacije civilnog društva, akademska zajednica, istraživačke organizacije, sindikati i organizacije za zaštitu potrošača u dizajnu i razvoju UI sustava te raznolikost razvojnih timova, uključujući ravnotežu spolova. Kako bi se osigurala djelotvornost dobrovoljnih kodeksa ponašanja, oni bi se trebali temeljiti na jasnim ciljevima i ključnim pokazateljima uspješnosti za mjerenje ostvarenja tih ciljeva. Trebalo bi ih također razvijati na uključiv način, prema potrebi, uz sudjelovanje relevantnih dionika kao što su poduzeća i organizacije civilnog društva, akademska zajednica, istraživačke organizacije, sindikati i organizacije za zaštitu potrošača. Komisija može osmisliti inicijative, među ostalim na sektorskoj razini, za olakšavanje smanjivanja tehničkih zapreka prekograničnoj razmjeni podataka u svrhu razvoja umjetne inteligencije, među ostalim i u području infrastrukture za pristup podacima te semantičke i tehničke interoperabilnosti različitih vrsta podataka.

- (166) Važno je da UI sustavi povezani s proizvodima koji nisu visokorizični u skladu s ovom Uredbom te stoga ne moraju ispunjavati zahtjeve utvrđene za visokorizične UI sustave ipak budu sigurni kad se stavljaju na tržište ili u upotrebu. Kako bi se doprinijelo tom cilju, Uredba (EU) 2023/988 Europskog parlamenta i Vijeća⁵³ primjenjivala bi se kao sigurnosni mehanizam.
- (167) Kako bi se osigurala pouzdana i konstruktivna suradnja nadležnih tijela na razini Unije i na nacionalnoj razini, sve strane uključene u primjenu ove Uredbe trebale bi poštovati povjerljivost informacija i podataka prikupljenih pri obavljanju svojih zadaća, u skladu s pravom Unije ili nacionalnim pravom. Svoje zadaće i aktivnosti trebale bi obavljati tako da osobito štite prava intelektualnog vlasništva, povjerljive poslovne informacije i poslovne tajne, djelotvornu provedbu ove Uredbe, javne i nacionalne sigurnosne interese, integritet kaznenih i upravnih postupaka te integritet klasificiranih podataka.

⁵³ Uredba (EU) 2023/988 Europskog parlamenta i Vijeća od 10. svibnja 2023. o općoj sigurnosti proizvoda, izmjeni Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća i Direktive (EU) 2020/1828 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2001/95/EZ Europskog parlamenta i Vijeća i Direktive Vijeća 87/357/EEZ (SL L 135, 23.5.2023., str. 1.).

- (168) Usklađenost s ovom Uredbom trebala bi biti izvršiva izricanjem sankcija i drugih mjera izvršavanja. Države članice trebale bi poduzeti sve mjere potrebne za osiguravanje provedbe odredaba ove Uredbe, među ostalim utvrđivanjem učinkovitih, proporcionalnih i odvrćajućih sankcija za povrede tih odredaba, i za poštovanje načela *ne bis in idem*. Kako bi se postrožile i uskladile upravne sankcije za povrede ove Uredbe, trebalo bi utvrditi gornje granice za određivanje upravnih novčanih kazni za određene specifične povrede. Pri procjeni iznosa novčanih kazni države članice trebale bi u svakom pojedinačnom slučaju uzeti u obzir sve relevantne okolnosti specifične situacije, posebno uzimajući u obzir prirodu, težinu i trajanje povrede i njezine posljedice te veličinu dobavljača, posebno ako je dobavljač MSP, uključujući *start-up* poduzeće. Europski nadzornik za zaštitu podataka trebao bi imati ovlast izreći novčane kazne institucijama, agencijama i tijelima Unije obuhvaćenima područjem primjene ove Uredbe.
- (169) Usklađenost s obvezama dobavljača UI modela opće namjene koje su propisane na temelju ove Uredbe trebala bi biti izvršiva, među ostalim, novčanim kaznama. U tu bi svrhu također trebalo utvrditi odgovarajuće razine novčanih kazni za povrede tih obveza, uključujući nepoštovanje mjera koje je Komisija zatražila u skladu s ovom Uredbom, podložno odgovarajućim rokovima zastare u skladu s načelom proporcionalnosti. Sve odluke koje Komisija donosi na temelju ove Uredbe podliježu postupku preispitivanja pred Sudom Europske unije u skladu s UFEU-om, među ostalim i neograničenoj nadležnosti Suda u pogledu sankcija u skladu s člankom 261. UFEU-a.

- (170) Pravom Unije i nacionalnim pravom već su predviđena djelotvorna pravna sredstva za fizičke i pravne osobe na čija prava i slobode negativno utječe upotreba UI sustavâ. Ne dovodeći u pitanje ta pravna sredstva, svaka fizička ili pravna osoba koja ima razloga smatrati da je došlo do povrede ove Uredbe trebala bi imati pravo podnijeti pritužbu relevantnom tijelu za nadzor tržišta.
- (171) Zahvaćene osobe trebale bi imati pravo dobiti objašnjenje ako se odluka subjekta koji uvodi sustav uglavnom temelji na izlaznim rezultatima iz određenih visokorizičnih UI sustava obuhvaćenih područjem primjene ove Uredbe i ako ta odluka proizvodi pravne učinke ili na sličan način znatno utječe na te osobe na način za koji smatraju da ima negativan učinak na njihovo zdravlje, sigurnost ili temeljna prava. To bi objašnjenje trebalo biti jasno i smisleno te bi trebalo biti osnova koja omogućuje zahvaćenim osobama da ostvare svoja prava. Pravo na dobivanje objašnjenja ne bi se trebalo primjenjivati na upotrebu UI sustava za koje iznimke ili ograničenja proizlaze iz prava Unije ili nacionalnog prava i trebalo bi se primjenjivati samo u mjeri u kojoj to pravo već nije predviđeno pravom Unije.
- (172) Osobe koje djeluju kao zviždači u vezi s povredama ove Uredbe trebale bi biti zaštićene pravom Unije. Direktiva (EU) 2019/1937 Europskog parlamenta i Vijeća⁵⁴ stoga bi se trebala primjenjivati na prijavljivanje povreda ove Uredbe i na zaštitu osoba koje prijavljuju te povrede.

⁵⁴ Direktiva (EU) 2019/1937 Europskog parlamenta i Vijeća od 23. listopada 2019. o zaštiti osoba koje prijavljuju povrede prava Unije (SL L 305, 26.11.2019., str. 17.).

(173) Kako bi se osiguralo da se regulatorni okvir može prilagođavati ako je to potrebno, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a radi izmjene uvjeta na temelju kojih se UI sustav ne treba smatrati visokorizičnim, popisa visokorizičnih UI sustava, odredaba o tehničkoj dokumentaciji, sadržaja EU izjave o sukladnosti, odredaba o postupcima ocjenjivanja sukladnosti, odredaba kojima se utvrđuju visokorizični UI sustavi na koje bi se trebao primjenjivati postupak ocjenjivanja sukladnosti na temelju ocjene sustava upravljanja kvalitetom i ocjene tehničke dokumentacije, praga, referentnih vrijednosti i pokazatelja, među ostalim dopunjavanjem tih referentnih vrijednosti i pokazatelja, u pravilima za klasifikaciju UI modela opće namjene sa sistemskim rizikom, kriterija za određivanje UI modela opće namjene sa sistemskim rizikom, tehničke dokumentacije za dobavljače UI modela opće namjene i informacija o transparentnosti za dobavljače UI modela opće namjene. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.⁵⁵. Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

⁵⁵ SL L 123, 12.5.2016., str. 1.

- (174) S obzirom na brz tehnološki razvoj i tehničko stručno znanje koje je potrebno za djelotvornu primjenu ove Uredbe, Komisija bi trebala evaluirati i preispitati ovu Uredbu do ... [pet godina od datuma stupanja na snagu ove Uredbe] i svake četiri godine nakon toga te o tome izvijestiti Europski parlament i Vijeće. Osim toga, uzimajući u obzir posljedice za područje primjene ove Uredbe, Komisija bi jednom godišnje trebala provesti procjenu potrebe za izmjenom popisa visokorizičnih UI sustava i popisa zabranjenih praksi. Nadalje, do ... [četiri godine od datuma stupanja na snagu ove Uredbe] i svake četiri godine nakon toga Komisija bi trebala evaluirati potrebu za izmjenom popisa naslova visokorizičnih područja iz priloga ovoj Uredbi, UI sustava obuhvaćenih obvezama transparentnosti, djelotvornosti sustava nadzora i upravljanja te napretka u razvoju normizacijskih dokumenata o energetske učinkovitom razvoju UI modela opće namjene, uključujući potrebu za daljnjim mjerama ili djelovanjima, te o tome izvijestiti Europski parlament i Vijeće. Naposljetku, do ... [četiri godine od datuma stupanja na snagu ove Uredbe] i svake tri godine nakon toga Komisija bi trebala evaluirati učinak i djelotvornost dobrovoljnih kodeksa ponašanja namijenjenih poticanju primjene zahtjeva predviđenih za visokorizične UI sustave u slučaju UI sustava koji nisu visokorizični i eventualno drugih dodatnih zahtjeva za takve UI sustave.

- (175) Radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe provedbene ovlasti trebalo bi dodijeliti Komisiji. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća⁵⁶.
- (176) S obzirom na to da cilj ove Uredbe, to jest poboljšanje funkcioniranja unutarnjeg tržišta i promicanje uvođenja antropocentrične umjetne inteligencije, uz istodobno osiguravanje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava sadržanih u Povelji, uključujući demokraciju, vladavinu prava i zaštitu okoliša od štetnih učinaka UI sustavâ u Uniji te podupiranje inovacija, ne mogu dostatno ostvariti države članice, nego se zbog opsega ili učinaka djelovanja on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. UEU-a. U skladu s načelom proporcionalnosti utvrđenim u tom članku ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

⁵⁶ Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

- (177) Kako bi se zajamčila pravna sigurnost, osiguralo odgovarajuće razdoblje prilagodbe za operatere i izbjegli poremećaji na tržištu, među ostalim osiguravanjem kontinuiteta korištenja UI sustavâ, primjereno je da se ova Uredba primjenjuje na visokorizične UI sustave koji su stavljeni na tržište ili u upotrebu prije općeg datuma početka njezine primjene samo ako od tog datuma u tim sustavima dođe do znatnih promjena u pogledu njihova dizajna ili namjene. Primjereno je pojasniti da bi u tom pogledu pojam znatne promjene trebalo razumjeti kao sadržajno jednakovrijedan pojmu znatne izmjene, koji se upotrebljava samo u pogledu visokorizičnih UI sustava na temelju ove Uredbe. Iznimno i s obzirom na javnu odgovornost, operateri UI sustava koji su komponente opsežnih informacijskih sustava uspostavljenih pravnim aktima navedenima u prilogu ovoj Uredbi i operateri visokorizičnih UI sustava namijenjenih korištenju od strane tijela javne vlasti trebali bi poduzeti potrebne korake kako bi ispunili zahtjeve iz ove Uredbe do kraja 2030. i do ... [šest godina od datuma stupanja na snagu ove Uredbe].
- (178) Dobavljače visokorizičnih UI sustava potiče se da dobrovoljno počnu ispunjavati relevantne obveze iz ove Uredbe već tijekom prijelaznog razdoblja.

- (179) Ova Uredba trebala bi se primjenjivati od ... [dvije godine od datuma stupanja na snagu ove Uredbe]. Međutim, uzimajući u obzir neprihvatljiv rizik povezan s korištenjem umjetne inteligencije na određene načine, zabrane kao i opće odredbe ove Uredbe trebale bi se trebale primjenjivati već od ... [šest mjeseci od datuma stupanja na snagu ove Uredbe]. Iako potpuni učinak tih zabrana proizlazi iz uspostave upravljanja i izvršavanja ove Uredbe, predviđanje primjene zabrana važno je kako bi se uzeli u obzir neprihvatljivi rizici i kako bi se utjecalo na druge postupke, primjerice u građanskom pravu.
- Nadalje, infrastruktura povezana s upravljanjem i sustavom za ocjenjivanje sukladnosti trebala bi biti spremna za upotrebu prije ... [dvije godine od datuma stupanja na snagu ove Uredbe], pa bi se stoga odredbe o prijavljenim tijelima i strukturama upravljanja trebale primjenjivati od ... [12 mjeseci od datuma stupanja na snagu ove Uredbe]. S obzirom na brz tehnološki napredak i usvajanje UI modelâ opće namjene, obveze dobavljača UI modelâ opće namjene trebale bi se primjenjivati od ... [12 mjeseci od datuma stupanja na snagu ove Uredbe]. Kodeksi prakse trebali bi biti spremni do ... [devet mjeseci od datuma stupanja na snagu ove Uredbe] kako bi se dobavljačima omogućilo da pravodobno dokažu usklađenost. Ured za umjetnu inteligenciju trebao bi osigurati da pravila i postupci klasifikacije budu ažurirani s obzirom na tehnološki razvoj. Usto, države članice trebale bi utvrditi pravila o sankcijama i obavijestiti Komisiju o tim pravilima, uključujući upravne novčane kazne, te osigurati njihovu pravilnu i djelotvornu provedbu do datuma početka primjene ove Uredbe. Stoga bi se odredbe o sankcijama trebale primjenjivati od ... [12 mjeseca od datuma stupanja na snagu ove Uredbe].

- (180) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka i s Europskim odborom za zaštitu podataka u skladu s člankom 42. stavcima 1. i 2. Uredbe (EZ) br. 2018/1725 te su oni dali zajedničko mišljenje 18. lipnja 2021.,

DONIJELI SU OVU UREDBU:

Poglavlje I.

Opće odredbe

Članak 1.

Predmet

1. Svrha je ove Uredbe poboljšati funkcioniranje unutarnjeg tržišta i promicati uvođenje antropocentrične i pouzdane umjetne inteligencije, uz istodobno osiguravanje visoke razine zaštite zdravlja, sigurnosti i temeljnih prava sadržanih u Povelji, uključujući demokraciju, vladavinu prava i zaštitu okoliša, od štetnih učinaka UI sustavâ u Uniji, te podupiranje inovacija.
2. Ovom se Uredbom utvrđuju:
 - (a) usklađena pravila za stavljanje na tržište, stavljanje u upotrebu i korištenje UI sustava u Uniji;
 - (b) zabrane određenih praksi u području umjetne inteligencije;
 - (c) posebni zahtjevi za visokorizične UI sustave i obveze za operatere takvih sustava;
 - (d) usklađena pravila o transparentnosti za određene UI sustave;
 - (e) usklađena pravila za stavljanje na tržište UI modelâ opće namjene;

- (f) pravila o praćenju tržišta, nadzoru tržišta, upravljanju i izvršavanju;
- (g) mjere za potporu inovacijama, posebno usmjerene na MSP-ove, uključujući *start-up* poduzeća.

Članak 2.

Područje primjene

1. Ova Uredba primjenjuje se na:

- (a) dobavljače koji stavljaju na tržište ili u upotrebu UI sustave ili stavljaju na tržište UI modele opće namjene u Uniji, bez obzira na to imaju li ti dobavljači poslovni nastan u Uniji ili u nekoj trećoj zemlji ili nalaze li se u Uniji ili u trećoj zemlji;
- (b) subjekte koji uvode UI sustave, a koji imaju poslovni nastan u Uniji ili se nalaze u Uniji;
- (c) dobavljače UI sustava i subjekte koji uvode UI sustave koji imaju poslovni nastan u trećoj zemlji ili se nalaze u trećoj zemlji ako se izlazni rezultati UI sustava upotrebljavaju u Uniji;
- (d) uvoznike i distributere UI sustavâ;
- (e) proizvođače proizvoda koji stavljaju na tržište ili u upotrebu UI sustav zajedno sa svojim proizvodom i pod vlastitim imenom ili žigom;
- (f) ovlaštene zastupnike dobavljača koji nemaju poslovni nastan u Uniji;
- (g) zahvaćene osobe koje se nalaze u Uniji.

2. Na UI sustave klasificirane kao visokorizične u skladu s člankom 6. stavkom 1. u odnosu na proizvode obuhvaćene zakonodavstvom Unije o usklađivanju navedenim u odjeljku B Priloga I. primjenjuju se samo članak 6. stavak 1., članci od 102. do 109. i članak 112. Članak 57. primjenjuje se samo u mjeri u kojoj su zahtjevi za visokorizične UI sustave iz ove Uredbe uključeni u to zakonodavstvo Unije o usklađivanju.
3. Ova se Uredba ne primjenjuje na područja izvan područja primjene prava Unije i ni u kojem slučaju ne utječe na nadležnosti država članica u pogledu nacionalne sigurnosti, bez obzira na vrstu subjekta kojem su države članice povjerile obavljanje zadaća u vezi s tim nadležnostima.
- Ova se Uredba ne primjenjuje na UI sustave ako i u mjeri u kojoj se stavljaju na tržište, u upotrebu ili upotrebljavaju s izmjenama ili bez njih isključivo u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću, bez obzira na vrstu subjekta koji obavlja te aktivnosti.
- Ova se Uredba ne primjenjuje na UI sustave koji se ne stavljaju na tržište ni u upotrebu u Uniji ako se izlazni rezultati upotrebljavaju u Uniji isključivo u vojne svrhe, obrambene svrhe ili u svrhe povezane s nacionalnom sigurnošću, bez obzira na vrstu subjekta koji obavlja te aktivnosti.

4. Ova se Uredba ne primjenjuje na tijela javne vlasti u trećoj zemlji ni na međunarodne organizacije obuhvaćene područjem primjene ove Uredbe na temelju stavka 1. ako ta tijela ili te organizacije upotrebljavaju UI sustave u okviru međunarodne suradnje ili sporazumâ o suradnji u području kaznenog progona i pravosudne suradnje s Unijom ili s jednom ili više država članica, pod uvjetom da takva treća zemlja ili međunarodna organizacija pruža odgovarajuće zaštitne mjere u pogledu zaštite temeljnih prava i sloboda pojedinaca.
5. Ova Uredba ne utječe na primjenu odredaba o odgovornosti pružatelja usluga posredovanja kako je utvrđeno u poglavlju II. Uredbe (EU) 2022/2065.
6. Ova Uredba ne primjenjuje se na UI sustave ili UI modele, uključujući njihove izlazne rezultate, koji su posebno razvijeni i stavljeni u upotrebu isključivo u svrhu znanstvenih istraživanja i razvoja.
7. Pravo Unije o zaštiti osobnih podataka, privatnosti i povjerljivosti komunikacija primjenjuje se na osobne podatke koji se obrađuju u vezi s pravima i obvezama utvrđenima u ovoj Uredbi. Ova Uredba ne utječe na uredbe (EU) 2016/679 i (EU) 2018/1725 ni na direktive 2002/58/EZ i (EU) 2016/680, ne dovodeći pritom u pitanje članak 10. stavak 5. i članak 59. ove Uredbe.
8. Ova se Uredba ne primjenjuje na aktivnosti istraživanja, testiranja ili razvoja UI sustava ili UI modela prije njihova stavljanja na tržište ili u upotrebu. Takve se aktivnosti provode u skladu s primjenjivim pravom Unije. Testiranje u stvarnim uvjetima nije obuhvaćeno tim isključenjem.

9. Ovom se Uredbom ne dovode u pitanje pravila utvrđena drugim pravnim aktima Unije povezanim sa zaštitom potrošača i sigurnošću proizvoda.
10. Ova se Uredba ne primjenjuje na obveze subjekata koji uvode sustav koji su fizičke osobe koje upotrebljavaju UI sustave isključivo u osobnoj neprofesionalnoj djelatnosti.
11. Ovom se Uredbom Uniju ili države članice ne sprečava da zadrže ili uvedu zakone i druge propise koji su pogodniji za radnike u smislu zaštite njihovih prava u pogledu korištenja UI sustava od strane poslodavaca, ili da potiču ili dopuštaju primjenu kolektivnih ugovora koji su pogodniji za radnike.
12. Ova se Uredba ne primjenjuje na UI sustave koji se objavljuju na temelju besplatnih licencija za softver otvorenog koda, osim ako se stavljaju na tržište ili u upotrebu kao visokorizični UI sustavi ili kao UI sustav obuhvaćen člankom 5. ili člankom 50.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „UI sustav” znači strojni sustav dizajniran za rad s promjenjivim razinama autonomije i koji nakon uvođenja može pokazati prilagodljivost te koji, za eksplicitne ili implicitne ciljeve, iz ulaznih vrijednosti koje prima, zaključuje kako generirati izlazne vrijednosti kao što su predviđanja, sadržaj, preporuke ili odluke koji mogu utjecati na fizička ili virtualna okruženja;

2. „rizik” znači kombinacija vjerojatnosti nastanka štete i težine te štete;
3. „dobavljač” znači fizička ili pravna osoba, tijelo javne vlasti, javna agencija ili drugo javno tijelo koje razvija UI sustav ili UI model opće namjene ili koji ima razvijen UI sustav ili UI model opće namjene i stavlja ga na tržište ili stavlja UI sustav u upotrebu pod vlastitim imenom ili žigom, uz plaćanje ili besplatno;
4. „subjekt koji uvodi sustav” znači fizička ili pravna osoba, tijelo javne vlasti, javna agencija ili drugo javno tijelo koje upotrebljava UI sustav u okviru svoje nadležnosti, osim ako se UI sustav upotrebljava u osobnoj neprofesionalnoj djelatnosti;
5. „ovlašteni zastupnik” znači fizička ili pravna osoba koja se nalazi u Uniji ili ima poslovni nastan u Uniji, koju je dobavljač UI sustava ili UI modela opće namjene pisanim putem ovlastio da u njegovo ime izvršava i provodi obveze i postupke utvrđene u ovoj Uredbi i koja je takvo ovlaštenje prihvatila;
6. „uvoznik” znači fizička ili pravna osoba koja se nalazi u Uniji ili ima poslovni nastan u Uniji i koja stavlja na tržište UI sustav s imenom ili žigom fizičke ili pravne osobe s poslovnim nastanom u trećoj zemlji;
7. „distributer” znači fizička ili pravna osoba u opskrbnom lancu koja nije dobavljač ni uvoznik i koja stavlja UI sustav na tržište Unije;
8. „operator” znači dobavljač, proizvođač proizvoda, subjekt koji uvodi sustav, ovlašteni zastupnik, uvoznik ili distributer;

9. „stavljanje na tržište” znači prvo stavljanje UI sustava ili UI modela opće namjene na raspolaganje na tržištu Unije;
10. „stavljanje na raspolaganje na tržištu” znači isporuka UI sustava ili UI modela opće namjene za distribuciju ili upotrebu na tržištu Unije u okviru komercijalne djelatnosti, uz plaćanje ili besplatno;
11. „stavljanje u upotrebu” znači isporuka UI sustava za prvu upotrebu u Uniji u skladu s njegovom namjenom izravno subjektu koji uvodi sustav ili za vlastite potrebe;
12. „namjena” znači korištenje za koje je dobavljač namijenio UI sustav, uključujući specifični kontekst i uvjete korištenja, kako je određeno u informacijama koje je dobavljač naveo u uputama za korištenje, promotivnim ili prodajnim materijalima i izjavama te u tehničkoj dokumentaciji;
13. „razumno predvidljiva pogrešna upotreba” znači upotreba UI sustava na način koji nije u skladu s njegovom namjenom, ali može biti posljedica razumno predvidljivog čovjekova ponašanja ili interakcije s drugim sustavima, uključujući druge UI sustave;
14. „sigurnosna komponenta” znači komponenta proizvoda ili UI sustava koja ima sigurnosnu funkciju u tom proizvodu ili UI sustavu ili čiji kvar ili neispravnost ugrožava zdravlje i sigurnost osoba ili imovine;
15. „upute za korištenje” znači informacije kojima dobavljač u prvom redu informira subjekt koji uvodi sustav o namjeni i pravilnom korištenju UI sustava;

16. „opoziv UI sustava” znači svaka mjera čiji je cilj postizanje vraćanja dobavljaču UI sustava stavljenog na raspolaganje subjektima koji uvode sustav ili njegovo izuzimanje iz usluge ili onemogućavanje njegova korištenja;
17. „povlačenje UI sustava” znači svaka mjera čiji je cilj sprečavanje da se UI sustav u opskrbnom lancu stavi na raspolaganje na tržištu;
18. „učinkovitost UI sustava” znači sposobnost UI sustava da ostvari svoju namjenu;
19. „tijelo koje provodi prijavljivanje” znači nacionalno tijelo odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, obavješćivanje i praćenje tijelâ za ocjenjivanje sukladnosti;
20. „ocjenjivanje sukladnosti” znači postupak kojim se dokazuje jesu li ispunjeni zahtjevi utvrđeni u poglavlju III. odjeljku 2. koji se odnose na visokorizični UI sustav;
21. „tijelo za ocjenjivanje sukladnosti” znači tijelo koje provodi aktivnosti ocjenjivanja sukladnosti kao treća strana, uključujući testiranje, certifikaciju i inspekciju;
22. „prijavljeno tijelo” znači tijelo za ocjenjivanje sukladnosti prijavljeno u skladu s ovom Uredbom i drugim relevantnim zakonodavstvom Unije o usklađivanju;
23. „bitna izmjena” znači promjena UI sustava nakon njegova stavljanja na tržište ili u upotrebu koja nije predviđena ili planirana u okviru početnog ocjenjivanja sukladnosti koje je proveo dobavljač i koja utječe na usklađenost UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2. ili koja prouzroči izmjenu namjene prema kojoj je UI sustav bio ocijenjen;

24. „oznaka CE” znači oznaka kojom dobavljač označuje da je UI sustav sukladan sa zahtjevima utvrđenima u poglavlju III. odjeljku 2. i drugim primjenjivim zakonodavstvom Unije o usklađivanju kojim se propisuje stavljanje te oznake;
25. „sustav praćenja nakon stavljanja na tržište” znači sve aktivnosti kojima dobavljači UI sustava prikupljaju i analiziraju iskustva stečena korištenjem UI sustava koje stavljaju na tržište ili u upotrebu kako bi utvrdili postoji li potreba za hitnim poduzimanjem eventualnih nužnih korektivnih ili preventivnih mjera;
26. „tijelo za nadzor tržišta” znači nacionalno tijelo koje provodi aktivnosti i poduzima mjere na temelju Uredbe (EU) 2019/1020;
27. „usklađena norma” znači usklađena norma kako je definirana u članku 2. stavku 1. točki (c) Uredbe (EU) br. 1025/2012;
28. „zajednička specifikacija” znači skup tehničkih specifikacija kako su definirane u članku 2. točki 4. Uredbe (EU) br. 1025/2012, kojim se pružaju sredstva za ispunjavanje određenih zahtjeva utvrđenih ovom Uredbom;
29. „podaci za treniranje” znači podaci koji se upotrebljavaju za treniranje UI sustava prilagođavanjem njegovih poučivih parametara;
30. „podaci za validaciju” znači podaci koji se upotrebljavaju za evaluaciju treniranog UI sustava te za ugađanje njegovih nepoučivih parametara i njegova procesa učenja kako bi se, među ostalim, izbjegla nedovoljna prilagodba ili prekomjerna prilagodba;

31. „skup podataka za validaciju” znači zaseban skup podataka ili fiksni ili varijabilni dio skupa podataka za treniranje;
32. „podaci za testiranje” znači podaci koji se upotrebljavaju za neovisnu evaluaciju UI sustava kako bi se potvrdila očekivana učinkovitost tog sustava prije njegova stavljanja na tržište ili u upotrebu;
33. „ulazni podaci” znači podaci koji su uneseni u UI sustav ili koje je UI sustav izravno stekao, a na temelju kojih sustav stvara izlazni rezultat;
34. „biometrijski podaci” znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim, fiziološkim i bihevioralnim obilježjima fizičke osobe, kao što su prikazi lica ili daktiloskopski podaci;
35. „biometrijska identifikacija” znači automatizirano prepoznavanje fizičkih, fizioloških, bihevioralnih ili psiholoških obilježja ljudi u svrhu utvrđivanja identiteta fizičke osobe usporedbom biometrijskih podataka tog pojedinca s biometrijskim podacima pojedinaca pohranjenima u bazi podataka;
36. „biometrijska provjera” znači automatizirana provjera usporedbom dvaju uzoraka, uključujući autentifikaciju, kojom se identitet fizičkih osoba provjerava usporedbom njihovih biometrijskih podataka s prethodno dostavljenim biometrijskim podacima;
37. „posebne kategorije osobnih podataka” znači kategorije osobnih podataka iz članka 9. stavka 1. Uredbe (EU) 2016/679, članka 10. Direktive (EU) 2016/680 i članka 10. stavka 1. Uredbe (EU) 2018/1725;

38. „osjetljivi operativni podaci” znači operativni podaci povezani s aktivnostima sprečavanja, otkrivanja, istrage ili progona kaznenih djela čije bi otkrivanje moglo ugroziti integritet kaznenog postupka;
39. „sustav za prepoznavanje emocija” znači UI sustav namijenjen prepoznavanju emocija ili namjera fizičkih osoba ili izvođenju zaključaka o njihovim emocijama ili namjerama na temelju njihovih biometrijskih podataka;
40. „sustav za biometrijsku kategorizaciju” znači UI sustav namijenjen razvrstavanju fizičkih osoba u određene kategorije na temelju njihovih biometrijskih podataka, osim ako je on pomoćni element druge komercijalne usluge i nužan iz objektivnih tehničkih razloga;
41. „sustav za daljinsku biometrijsku identifikaciju” znači UI sustav namijenjen identifikaciji fizičkih osoba, bez njihova aktivnog sudjelovanja, obično na daljinu usporedbom biometrijskih podataka dotične osobe s biometrijskim podacima iz referentne baze podataka;
42. „sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu” znači sustav za daljinsku biometrijsku identifikaciju koji bez većeg kašnjenja prikuplja biometrijske podatke, vrši usporedbe i provodi identifikaciju, a obuhvaća ne samo trenutačnu identifikaciju nego i ograničena manja kašnjenja kako bi se izbjeglo zaobilaženje propisa;
43. „sustav za naknadnu daljinsku biometrijsku identifikaciju” znači sustav za daljinsku biometrijsku identifikaciju koji nije sustav za daljinsku biometrijsku identifikaciju u stvarnom vremenu;

44. „javno mjesto” znači svako fizičko mjesto u javnom ili privatnom vlasništvu dostupno neodređenom broju fizičkih osoba, bez obzira na to primjenjuju li se određeni uvjeti za pristup i bez obzira na moguća ograničenja kapaciteta;
45. „tijelo kaznenog progona” znači:
- (a) svako tijelo javne vlasti nadležno za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili izvršenje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje; ili
 - (b) svako drugo tijelo ili subjekt kojem je pravom države članice povjereno izvršavanje javne vlasti i javnih ovlasti u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
46. „kazneni progon” znači aktivnosti koje provode tijela kaznenog progona ili koje se provode u njihovo ime radi sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje;
47. „Ured za umjetnu inteligenciju” znači Komisijina funkcija doprinošenja provedbi, praćenju i nadzoru UI sustavâ i UI modelâ opće namjene i upravljanju umjetnom inteligencijom koja je predviđena u Odluci Komisije od 24. siječnja 2024.; upućivanja na Ured za umjetnu inteligenciju u ovoj Uredbi tumače se kao upućivanja na Komisiju;

48. „nacionalno nadležno tijelo” znači tijelo koje provodi prijavljivanje ili tijelo za nadzor tržišta; kad je riječ o UI sustavima koje stavljaju u uporabu ili koriste institucije, agencije, uredi i tijela Unije, upućivanja na nacionalna nadležna tijela ili tijela za nadzor tržišta u ovoj Uredbi smatraju se upućivanjima na Europskog nadzornika za zaštitu podataka;
49. „ozbiljan incident” znači incident ili neispravnost UI sustava koji su izravno ili neizravno doveli do bilo kojeg od sljedećeg:
- (a) smrti osobe ili ozbiljnog narušavanja zdravlja osobe;
 - (b) ozbiljnog i nepovratnog poremećaja u upravljanju kritičnom infrastrukturuom ili njezinu radu;
 - (c) povrede obveza na temelju prava Unije namijenjenih zaštiti temeljnih prava;
 - (d) teške štete za imovinu ili okoliš;
50. „osobni podaci” znači osobni podaci kako su definirani u članku 4. točki 1. Uredbe (EU) 2016/679;
51. „neosobni podaci” znači podaci koji nisu osobni podaci kako su definirani u članku 4. točki 1. Uredbe (EU) 2016/679;
52. „izrada profila” znači izrada profila kako je definirana u članku 4. točki 4. Uredbe (EU) 2016/679;

53. „plan testiranja u stvarnim uvjetima” znači dokument u kojem se opisuju ciljevi, metodologija, geografski, populacijski i vremenski opseg, praćenje, organizacija i provedba testiranja u stvarnim uvjetima;
54. „plan izoliranog okruženja” znači dokument koji su usuglasili uključeni dobavljač i nadležno tijelo, a u kojem se opisuju ciljevi, uvjeti, vremenski okvir, metodologija i zahtjevi za aktivnosti koje se provode u izoliranom okruženju;
55. „regulatorno izolirano okruženje za umjetnu inteligenciju” znači kontroliran okvir koji je uspostavilo nadležno tijelo i kojim se dobavljačima ili potencijalnim dobavljačima UI sustava nudi mogućnost razvoja, treniranja, validacije i testiranja inovativnog UI sustava, po mogućnosti u stvarnim uvjetima, u skladu s planom izoliranog okruženja, na ograničeno vrijeme i pod regulatornim nadzorom;
56. „pismenost u području umjetne inteligencije” znači vještine, znanje i razumijevanje koji dobavljačima, subjektima koji uvode sustav i zahvaćenim osobama omogućuju, uzimajući u obzir njihova prava i obveze u kontekstu ove Uredbe, da informirano uvode UI sustave, kao i da steknu svijest o mogućnostima i rizicima umjetne inteligencije te šteti koju može izazvati;
57. „testiranje u stvarnim uvjetima” znači privremeno testiranje UI sustava u odnosu na njegovu namjenu u stvarnim uvjetima izvan laboratorija ili u na drugi način simuliranom okruženju radi prikupljanja pouzdanih i čvrstih podataka te ocjenjivanja i provjere sukladnosti UI sustava sa zahtjevima ove Uredbe te se ne smatra stavljanjem UI sustava na tržište ili u upotrebu u smislu ove Uredbe, pod uvjetom da su ispunjeni svi uvjeti utvrđeni u članku 57. ili članku 60.;

58. „ispitanik” za potrebe testiranja u stvarnim uvjetima znači fizička osoba koja sudjeluje u testiranju u stvarnim uvjetima;
59. „informirani pristanak” znači ispitanikov slobodan, specifičan, nedvosmislen i dobrovoljan iskaz spremnosti da sudjeluje u određenom testiranju u stvarnim uvjetima nakon što je obaviješten o svim aspektima testiranja relevantnima za njegovu odluku o sudjelovanju;
60. „uvjerljiv krivotvoreni sadržaj (deep fake)” znači slike, audiosadržaj ili videosadržaj koji generira ili kojim manipulira umjetna inteligencija, a koji nalikuje stvarnim osobama, predmetima, mjestima, subjektima ili događajima i koji bi se nekome lažno činio vjerodostojnim ili istinitim;
61. „raširena povreda” znači svaki čin ili propust protivan pravu Unije kojim se štite interesi pojedinaca, a:
- (a) kojim je nanescena ili će vjerojatno biti nanescena šteta kolektivnim interesima pojedinaca koji borave u najmanje dvjema državama članicama koje nisu država članica:
 - i. u kojoj je čin ili propust nastao ili se dogodio;
 - ii. u kojoj se dotični dobavljač ili, ako je primjenjivo, njegov ovlašteni zastupnik nalazi ili ima poslovni nastan; ili
 - iii. u kojoj subjekt koji uvodi sustav ima poslovni nastan ako je povredu počinio taj subjekt;

(b) koji je uzrokovao, uzrokuje ili će vjerojatno uzrokovati nanošenje štete kolektivnim interesima pojedinaca i koji ima zajednička obilježja, uključujući istu nezakonitu praksu ili povredu istog interesa, i koji je istodobno počinio isti operater u najmanje trima državama članicama;

62. „kritična infrastruktura” znači kritična infrastruktura kako je definirana u članku 2. točki 4. Direktive (EU) 2022/2557;
63. „UI model opće namjene” znači UI model, uključujući takav UI model treniran s pomoću velike količine podataka uz primjenu samostalnog nadzora u širokim razmjerima, koji ima vrlo općenitu namjenu i može kompetentno obavljati širok raspon različitih zadataka bez obzira na način na koji se model stavlja na tržište i koji se može integrirati u razne sustave ili primjene niže u lancu, osim UI modela koji se upotrebljavaju za aktivnosti istraživanja, razvoja ili izrade prototipova prije njihova stavljanja na tržište;
64. „sposobnosti visokog učinka” znači sposobnosti koje odgovaraju sposobnostima zabilježenima kod najnaprednijih UI modela opće namjene ili ih nadilaze;
65. „sistemska rizik” znači rizik specifičan za sposobnosti visokog učinka UI modela opće namjene, koji ima znatan utjecaj na tržište Unije zbog svojeg dosega ili zbog stvarnih ili razumno predvidljivih negativnih učinaka na javno zdravlje, sigurnost, javnu sigurnost, temeljna prava ili društvo u cjelini, a koji se može proširiti po cijelom vrijednosnom lancu;

66. „UI sustav opće namjene” znači UI sustav koji se temelji na UI modelu opće namjene i koji može služiti različitim namjenama, ili za izravnu upotrebu ili za integraciju u druge UI sustave;
67. „matematička operacija nad brojevima s pomičnim zarezom” znači svaka matematička operacija ili dodjela koja uključuje brojeve s pomičnim zarezom, koji su podskup realnih brojeva koji su na računalima obično predstavljeni kao cijeli broj fiksne preciznosti skaliran cjelobrojnim eksponentom fiksne baze;
68. „dobavljač niže u lancu” znači dobavljač UI sustava, uključujući UI sustav opće namjene, u koji je integriran UI model, bez obzira na to dobavlja li UI model on sâm i je li vertikalno integriran ili ga dobavlja drugi subjekt na temelju ugovornih odnosa.

Članak 4.

Pismenost u području umjetne inteligencije

Dobavljači i subjekti koji uvode UI sustave poduzimaju mjere kako bi na najbolji mogući način osigurali dostatnu razinu pismenosti u području umjetne inteligencije za svoje osoblje i druge osobe uključene u rad i korištenje UI sustava u njihovo ime, uzimajući u obzir njihovo tehničko znanje, iskustvo, obrazovanje i osposobljavanje te kontekst u kojem će se UI sustavi koristiti, kao i osobe ili skupine osoba na kojima se UI sustavi trebaju upotrijebiti.

Poglavlje II.

Zabranjene prakse u području umjetne inteligencije

Članak 5.

Zabranjene prakse u području umjetne inteligencije

1. Zabranjuju se sljedeće prakse u području umjetne inteligencije:
 - (a) stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava u kojem se primjenjuju subliminalne tehnike kojih osoba nije svjesna ili namjerno manipulativne ili obmanjujuće tehnike s ciljem ili s učinkom bitnog iskrivljavanja ponašanja osobe ili skupine osoba tako da se znatno narušava njihova sposobnost da donesu informiranu odluku, zbog čega donose odluku koju inače ne bi donijele, na način kojim se toj osobi, drugoj osobi ili skupini osoba uzrokuje znatna šteta ili se može razumno očekivati da će se prouzročiti takva šteta;
 - (b) stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava koji iskorištava bilo koju slabost fizičke osobe ili određene skupine osoba zbog njihove dobi, invaliditeta ili specifičnog društvenog ili ekonomskog položaja s ciljem ili s učinkom bitnog iskrivljavanja ponašanja te osobe ili osobe koja pripada toj skupini na način kojim se toj osobi ili nekoj drugoj osobi uzrokuje znatna šteta ili se može razumno očekivati da će se prouzročiti takva šteta;

- (c) stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava radi evaluacije ili klasifikacije fizičkih osoba ili skupina osoba tijekom određenog razdoblja na temelju njihova društvenog ponašanja ili poznatih, izvedenih ili predviđenih osobnih obilježja ili obilježja ličnosti, pri čemu njihov društveni rejting uzrokuje barem jedno od sljedećeg:
- i. štetno ili nepovoljno postupanje prema određenim fizičkim osobama ili skupinama osoba u društvenim kontekstima koji nisu povezani s kontekstima u kojima su podaci izvorno generirani ili prikupljeni;
 - ii. štetno ili nepovoljno postupanje prema određenim fizičkim osobama ili skupinama osoba koje je neopravdano ili nerazmjerno njihovu društvenom ponašanju ili njegovoj ozbiljnosti;
- (d) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava za procjene rizika u pogledu fizičkih osoba kako bi se procijenio ili predvidjeo rizik da će fizička osoba počiniti kazneno djelo, isključivo na temelju izrade profila fizičke osobe ili procjene njezinih osobina i obilježja ličnosti; ta se zabrana ne primjenjuje na UI sustave koji se upotrebljavaju za potporu ljudskoj procjeni uključenosti osobe u kriminalnu aktivnost, koja se već temelji na objektivnim i provjerljivim činjenicama izravno povezanim s kriminalnom aktivnošću;
- (e) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava koji stvaraju ili proširuju baze podataka za prepoznavanje lica neciljanim prikupljanjem fotografija lica s interneta ili snimki CCTV-a;

- (f) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili korištenje UI sustava za izvođenje zaključaka o emocijama fizičke osobe na radnome mjestu i u obrazovnim ustanovama, osim ako se UI sustav namjerava staviti u upotrebu ili na tržište iz medicinskih ili sigurnosnih razloga;
- (g) stavljanje na tržište, stavljanje u upotrebu u tu specifičnu svrhu ili upotreba sustavâ za biometrijsku kategorizaciju u kojima se fizičke osobe pojedinačno kategoriziraju na temelju njihovih biometrijskih podataka kako bi se zaključilo ili izvelo zaključke o njihovoj rasi, političkim mišljenjima, članstvu u sindikatu, vjerskim ili filozofskim uvjerenjima, spolnom životu ili seksualnoj orijentaciji; ta zabrana ne obuhvaća označivanje ili filtriranje zakonito pribavljenih biometrijskih skupova podataka, kao što su slike, na temelju biometrijskih podataka ili kategorizacije biometrijskih podataka u području kaznenog progona;
- (h) upotreba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona, osim ako je takva upotreba nužna i u mjeri u kojoj je nužna radi jednog od sljedećih ciljeva:
 - i. ciljane potrage za konkretnim žrtvama otmice, trgovine ljudima ili seksualnog iskorištavanja ljudi, kao i potrage za nestalim osobama;
 - ii. sprečavanja konkretne, znatne i izravne prijetnje životu ili tjelesnoj sigurnosti fizičkih osoba ili stvarne i prisutne ili stvarne i predvidljive prijetnje od terorističkog napada;

- iii. lociranja ili identifikacije osobe osumnjičene za počinjenje kaznenog djela u svrhu vođenja kaznene istrage ili progona ili izvršenja kaznene sankcije za kaznena djela iz Priloga II. za koja je u dotičnoj državi članici zapriječena kazna zatvora ili oduzimanja slobode u maksimalnom trajanju od najmanje četiri godine.

Prvim podstavkom točkom (h) ne dovodi se u pitanje članak 9. Uredbe (EU) 2016/679 kad je riječ o obradi biometrijskih podataka u svrhe koje nisu kazneni progon.

- 2. Upotreba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona radi bilo kojeg od ciljeva iz stavka 1. prvog podstavka točke (h) smije se uvesti u svrhe utvrđene u toj točki samo kako bi se potvrdio identitet konkretno ciljanog pojedinca, pri čemu se uzimaju u obzir sljedeći elementi:
 - (a) priroda situacije zbog koje se pojavila mogućnost upotrebe, osobito težina, vjerojatnost i razmjer štete koja bi nastala da se sustav ne koristi;
 - (b) posljedice upotrebe sustava na prava i slobode svih dotičnih osoba, osobito težina, vjerojatnost i razmjer tih posljedica.

Usto, upotreba sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona radi bilo kojeg od ciljeva iz stavka 1. prvog podstavka točke (h) ovog članka mora biti u skladu s potrebnim i razmjernim zaštitnim mjerama i uvjetima korištenja u skladu s nacionalnim pravom kojim se odobrava njihova upotreba, osobito u pogledu vremenskih i zemljopisnih ograničenja i ograničenja u pogledu osoba. Upotrebu sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima odobrava se samo ako je tijelo kaznenog progona dovršilo procjenu učinka na temeljna prava kako je predviđeno u članku 27. i registriralo sustav u bazi podataka EU-a u skladu s člankom 49. Međutim, u propisno opravdanim hitnim slučajevima takvi se sustavi mogu početi upotrebljavati bez registracije u bazi podataka EU-a, pod uvjetom da se takva registracija dovrši bez nepotrebne odgode.

3. Za potrebe stavka 1. prvog podstavka točke (h) i stavka 2., za svaku upotrebu sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona potrebno je prethodno odobrenje pravosudnog tijela ili neovisnog upravnog tijela čija je odluka obvezujuća iz države članice u kojoj će se sustav upotrebljavati, a koje se izdaje na obrazloženi zahtjev i u skladu s detaljnim pravilima nacionalnog prava iz stavka 5. Međutim, u propisno opravdanim hitnim situacijama takav se sustav može početi upotrebljavati bez odobrenja, pod uvjetom da se takvo odobrenje zatraži bez nepotrebne odgode, a najkasnije u roku od 24 sata. Ako je takvo odobrenje odbijeno, upotreba se smjesta zaustavlja te se svi podaci, kao i rezultati i izlazni podaci te upotrebe odmah odbacuju i brišu.

Nadležno pravosudno tijelo ili neovisno upravno tijelo čija je odluka obvezujuća izdaje odobrenje samo ako je uvjereno, na temelju objektivnih dokaza ili jasnih informacija koje su mu predložene, da je upotreba dotičnog sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu potrebna za postizanje jednog od ciljeva iz stavka 1. prvog podstavka točke (h) navedenog u zahtjevu i razmjerna tom cilju, a ponajprije ostaje ograničena na ono što je nužno kad je riječ o razdoblju te zemljopisnom i personalnom području primjene. Pri odlučivanju o zahtjevu to tijelo uzima u obzir elemente iz stavka 2. Odluka koja proizvodi negativan pravni učinak na osobu ne smije se donijeti isključivo na temelju izlaznih podataka sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu.

4. Ne dovodeći u pitanje stavak 3., o svakoj upotrebi sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona obavješćuju se relevantno tijelo za nadzor tržišta i nacionalno tijelo za zaštitu podataka u skladu s nacionalnim pravilima iz stavka 5. Obavijest mora sadržavati barem informacije navedene u stavku 6. i ne smije uključivati osjetljive operativne podatke.

5. Država članica može odlučiti predvidjeti mogućnost potpunog ili djelomičnog odobravanja upotrebe sustava za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona uz ograničenja i pod uvjetima iz stavka 1. prvog podstavka točke (h) te stavaka 2. i 3. Dotična država članica u svojem nacionalnom pravu utvrđuje potrebna detaljna pravila o podnošenju zahtjeva za odobrenja iz stavka 3., o izdavanju, izvršenju i nadzoru tih odobrenja te izvješćivanju u vezi s njima. U tim se pravilima također određuje za koje se ciljeve iz stavka 1. prvog podstavka točke (h), među ostalim i za koja kaznena djela iz njegove točke (h) podtočke iii., nadležnim tijelima može odobriti upotreba tih sustava u svrhu kaznenog progona. Države članice priopćuju Komisiji ta pravila najkasnije 30 dana nakon njihova donošenja. Države članice mogu, u skladu s pravom Unije, uvesti restriktivnije propise o upotrebi sustavâ za daljinsku biometrijsku identifikaciju.
6. Nacionalna tijela za nadzor tržišta i nacionalna tijela za zaštitu podataka država članica koja su obaviještena o upotrebi sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona na temelju stavka 4. podnose Komisiji godišnja izvješća o takvoj upotrebi. U tu svrhu Komisija državama članicama i nacionalnim tijelima za nadzor tržišta i zaštitu podataka dostavlja predložak, uključujući informacije o broju odluka koje su nadležna pravosudna tijela ili neovisno upravno tijelo čija je odluka obvezujuća donijeli na temelju zahtjevâ za izdavanje odobrenja u skladu sa stavkom 3. i njihov rezultat.

7. Komisija objavljuje godišnja izvješća o upotrebi sustavâ za daljinsku biometrijsku identifikaciju u stvarnom vremenu na javnim mjestima u svrhu kaznenog progona na temelju agregiranih podataka u državama članicama i godišnjih izvješća iz stavka 6. Ta godišnja izvješća ne smiju uključivati osjetljive operativne podatke o povezanim aktivnostima kaznenog progona.
8. Ovaj članak ne utječe na zabrane koje se primjenjuju ako se praksom u području umjetne inteligencije krši drugo pravo Unije.

Poglavlje III.

Visokorizični UI sustavi

ODJELJAK 1.

KLASIFIKACIJA UI SUSTAVA KAO VISOKORIZIČNIH

Članak 6.

Pravila o klasifikaciji UI sustava kao visokorizičnih

1. Bez obzira na to stavlja li se UI sustav na tržište ili u upotrebu neovisno o proizvodima iz točaka (a) i (b) taj se UI sustav smatra visokorizičnim ako su ispunjena oba sljedeća uvjeta:
 - (a) UI sustav namijenjen je za korištenje kao sigurnosna komponenta proizvoda ili je UI sustav sam po sebi proizvod koji je obuhvaćen zakonodavstvom Unije o usklađivanju navedenim u Prilogu I.;

- (b) za proizvod čija je sigurnosna komponenta na temelju točke (a) UI sustav ili UI sustav koji je sam po sebi proizvod zahtijeva se ocjenjivanje sukladnosti koje provodi treća strana radi stavljanja na tržište ili stavljanja u upotrebu tog proizvoda na temelju zakonodavstva Unije o usklađivanju navedenog u Prilogu I.
- 2. Uz visokorizične UI sustave iz stavka 1., u visokorizične sustave ubrajaju se UI sustavi iz Priloga III.
- 3. Odstupajući od stavka 2., UI sustav iz Priloga III. ne smatra se visokorizičnim ako ne predstavlja znatan rizik od štete za zdravlje, sigurnost ili temeljna prava fizičkih osoba, među ostalim ako bitno ne utječe na ishod donošenja odluka.

Prvi podstavak primjenjuje se ako je ispunjen bilo koji od sljedećih uvjeta:

- (a) UI sustav namijenjen je obavljanju uske postupovne zadaće;
- (b) UI sustav namijenjen je poboljšanju rezultata prethodno dovršene ljudske aktivnosti;
- (c) UI sustav namijenjen je otkrivanju obrazaca donošenja odluka ili odstupanja od ranijih obrazaca donošenja odluka i ne bi trebao zamijeniti prethodno dovršenu ljudsku procjenu niti na nju utjecati, bez odgovarajućeg preispitivanja koje provodi čovjek; ili
- (d) UI sustav namijenjen je obavljanju pripremne zadaće za ocjenjivanje relevantno za slučajeve upotrebe navedene u Prilogu III.

Ne dovodeći u pitanje prvi podstavak, UI sustav iz Priloga III. uvijek se smatra visokorizičnim ako taj UI sustav izrađuje profile fizičkih osoba.

4. Dobavljač koji smatra da UI sustav iz Priloga III. nije visokorizičan dokumentira svoje ocjenjivanje prije stavljanja tog sustava na tržište ili u upotrebu. Takav dobavljač podliježe obvezi registracije utvrđenoj u članku 49. stavku 2. Na zahtjev nacionalnih nadležnih tijela dobavljač dostavlja dokumentaciju o ocjenjivanju.
5. Komisija, nakon savjetovanja s Europskim vijećem za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”), a najkasnije ... [18 mjeseci od datuma stupanja na snagu ove Uredbe], izdaje smjernice u kojima se utvrđuje praktična provedba ovog članka u skladu s člankom 96. zajedno sa sveobuhvatnim popisom praktičnih slučajeva upotrebe UI sustava koji su visokorizični i koji nisu visokorizični.
6. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene stavka 3. drugog podstavka ovog članka dodavanjem novih uvjeta uvjetima koji su utvrđeni u stavku 3. drugom podstavku ovog članka ili mijenjanjem tih uvjeta ako postoje konkretni i pouzdani dokazi o postojanju UI sustava koji su obuhvaćeni područjem primjene Priloga III., ali ne predstavljaju znatan rizik od štete za zdravlje, sigurnost ili temeljna prava fizičkih osoba.

7. Komisija donosi delegirane akte u skladu s člankom 97. radi izmjene stavka 3. drugog podstavka ovog članka brisanjem bilo kojeg od uvjeta utvrđenih u stavku 3. drugom podstavku ovog članka ako postoje konkretni i pouzdani dokazi da je to potrebno radi održavanja razine zaštite zdravlja, sigurnosti i temeljnih prava koja je predviđena ovom Uredbom.
8. Nijednom izmjenom uvjeta utvrđenih u stavku 3. drugom podstavku donesenom u skladu sa stavcima 6. i 7. ovog članka ne smije se smanjiti ukupna razina zaštite zdravlja, sigurnosti i temeljnih prava koja je predviđena ovom Uredbom te se njome mora osigurati usklađenost s delegiranim aktima donesenima na temelju članka 7. stavka 1. i uzeti u obzir tržišni i tehnološki razvoj.

Članak 7.

Izmjene Priloga III.

1. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene Priloga III. dodavanjem ili prilagodbom slučajeva upotrebe visokorizičnih UI sustava ako su ispunjena oba sljedeća uvjeta:
 - (a) UI sustavi namijenjeni su za korištenje u bilo kojem od područja iz Priloga III.;
 - (b) UI sustavi predstavljaju rizik od štete za zdravlje i sigurnost ili rizik od nepovoljnog utjecaja na temeljna prava, a taj je rizik jednakovrijedan riziku ili veći od rizika od štete ili nepovoljnog utjecaja koji predstavljaju visokorizični UI sustavi već navedeni u Prilogu III.

2. Pri procjeni uvjeta iz stavka 1. točke (b) Komisija uzima u obzir sljedeće kriterije:
- (a) namjenu UI sustava;
 - (b) stupanj u kojem se UI sustav upotrebljava ili će se vjerojatno upotrebljavati;
 - (c) prirodu i količinu podataka koje obrađuje i upotrebljava UI sustav, a posebice obrađuju li se posebne kategorije osobnih podataka;
 - (d) stupanj u kojem UI sustav djeluje autonomno i mogućnost da čovjek nadjača odluku ili preporuke koje bi mogle prouzročiti štetu;
 - (e) stupanj u kojem je upotreba UI sustava već prouzročila štetu za zdravlje ili sigurnost ili imala nepovoljan utjecaj na temeljna prava ili izazvala ozbiljnu zabrinutost da bi mogla prouzročiti takvu štetu ili nepovoljan utjecaj, kako je, primjerice, potvrđeno u izvješćima ili dokumentiranim navodima koji su podneseni nacionalnim nadležnim tijelima ili u drugim izvješćima, ovisno o slučaju;
 - (f) potencijalne razmjere takve štete ili takvog nepovoljnog utjecaja, osobito u smislu intenziteta i mogućnosti da pogodi više osoba ili da nerazmjerno pogodi određenu skupinu osoba;
 - (g) stupanj u kojem potencijalno oštećene osobe ili osobe izložene nepovoljnom utjecaju ovise o ishodu upotrebe UI sustava, osobito ako taj ishod nije razumno moguće ne prihvatiti zbog praktičnih ili pravnih razloga;

- (h) stupanj u kojem postoji neravnoteža moći ili su potencijalno oštećene osobe ili osobe izložene nepovoljnom utjecaju u ranjivu položaju u odnosu na subjekt koji uvodi UI sustav, osobito zbog statusa, autoriteta, znanja, ekonomskih ili socijalnih okolnosti ili dobi;
- (i) stupanj u kojem je ishod nastao upotrebom UI sustava lako ispravljiv ili poništiv, uzimajući u obzir tehnička rješenja dostupna za njegovo ispravljanje ili poništenje, pri čemu se smatra da ishodi koji nepovoljno utječu na zdravlje, sigurnost ili temeljna prava nisu lako ispravljivi ili poništivi;
- (j) razmjer i vjerojatnost koristi od uvođenja UI sustava za pojedince, skupine ili društvo u cjelini, uključujući moguća poboljšanja sigurnosti proizvoda;
- (k) stupanj u kojem se postojećim pravom Unije predviđaju:
 - i. djelotvorne mjere pravne zaštite od rizika koji predstavlja UI sustav, uz iznimku zahtjeva za naknadu štete;
 - ii. djelotvorne mjere za sprečavanje ili što veće smanjenje tih rizika.

3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene popisa iz Priloga III. uklanjanjem visokorizičnih UI sustava ako su ispunjena oba sljedeća uvjeta:
- (a) dotični visokorizični UI sustav više ne predstavlja znatan rizik za temeljna prava, zdravlje ili sigurnost, uzimajući u obzir kriterije navedene u stavku 2.;
 - (b) brisanjem se ne smanjuje ukupna razina zaštite zdravlja, sigurnosti i temeljnih prava na temelju prava Unije.

ODJELJAK 2.

ZAHTJEVI ZA VISOKORIZIČNE UI SUSTAVE

Članak 8.

Ispunjavanje zahtjeva

1. Visokorizični UI sustavi mora ispunjavati zahtjeve utvrđene u ovom odjeljku, uzimajući u obzir njihovu namjenu i općepriznata najnovija dostignuća u području umjetne inteligencije i tehnologija povezanih s umjetnom inteligencijom. Pri osiguravanju ispunjavanja tih zahtjeva u obzir se uzima sustav upravljanja rizikom iz članka 9.

2. Ako proizvod sadržava UI sustav na koji se primjenjuju zahtjevi ove Uredbe i zahtjevi zakonodavstva Unije o usklađivanju iz odjeljka A Priloga I., dobavljači su odgovorni za osiguravanje potpune usklađenosti njihova proizvoda sa svim primjenjivim zahtjevima na temelju primjenjivog zakonodavstva Unije o usklađivanju. Pri osiguravanju usklađenosti visokorizičnih UI sustava iz stavka 1. sa zahtjevima utvrđenima u ovom odjeljku te kako bi se osigurala dosljednost, izbjeglo udvostručavanje i na najmanju moguću mjeru svela dodatna opterećenja, dobavljači imaju mogućnost da potrebne postupke testiranja i izvješćivanja, informacije i dokumentaciju koje pružaju u vezi sa svojim proizvodom prema potrebi integriraju u dokumentaciju i postupke koji već postoje i koji se zahtijevaju na temelju zakonodavstva Unije o usklađivanju navedenog u odjeljku A Priloga I.

Članak 9.

Sustav upravljanja rizikom

1. Za visokorizične UI sustave uspostavlja se, primjenjuje i održava sustav upravljanja rizikom te se o njemu vodi dokumentacija.
2. Sustav upravljanja rizikom shvaća se kao kontinuiran iterativan proces koji se planira i izvodi tijekom cijelog životnog ciklusa visokorizičnog UI sustava i koji je potrebno redovito i sustavno preispitivati i ažurirati. Obuhvaća sljedeće korake:
 - (a) utvrđivanje i analizu poznatih i razumno predvidljivih rizika koje visokorizični UI sustav može predstavljati za zdravlje, sigurnost ili temeljna prava kada se visokorizični UI sustav koristi u skladu sa svojom namjenom;

- (b) procjenjivanje i evaluaciju rizika koji mogu nastati pri korištenju visokorizičnog UI sustava u skladu s njegovom namjenom i u uvjetima razumno predvidljive pogrešne upotrebe;
 - (c) evaluaciju drugih potencijalnih rizika na temelju analize podataka prikupljenih sustavom praćenja nakon stavljanja na tržište iz članka 72.;
 - (d) donošenje odgovarajućih i ciljanih mjera upravljanja rizikom osmišljenih za uklanjanje rizika utvrđenih na temelju točke (a).
3. Rizici iz ovog članka odnose se samo na one rizike koji se mogu razumno ublažiti ili ukloniti razvijanjem ili dizajnom visokorizičnog UI sustava ili pružanjem adekvatnih tehničkih informacija.
4. U mjerama upravljanja rizikom iz stavka 2. točke (d) na odgovarajući način uzimaju se u obzir učinci i moguća interakcija koji proizlaze iz kombinirane primjene zahtjeva utvrđenih u ovom odjeljku, u cilju djelotvornijeg svođenja rizika na najmanju moguću mjeru i istodobnog postizanja odgovarajuće ravnoteže u provedbi mjera za ispunjavanje tih zahtjeva.
5. Mjere upravljanja rizikom iz stavka 2. točke (d) takve su da su relevantni preostali rizik povezan sa svakom pojedinom opasnošću kao i cjelokupni preostali rizik visokorizičnih UI sustava procijenjeni prihvatljivima.

Pri utvrđivanju najprikladnijih mjera upravljanja rizikom osigurava se sljedeće:

- (a) uklanjanje ili smanjenje rizika utvrđenih i evaluiranih na temelju stavka 2. u mjeri u kojoj je to tehnički izvedivo putem adekvatnog dizajna i razvoja visokorizičnog UI sustava;
- (b) prema potrebi, provedba adekvatnih mjera za ublažavanje i kontrolu rizika koji se ne mogu ukloniti;
- (c) pružanje informacija koje se zahtijevaju u skladu s člankom 13. i, prema potrebi, osposobljavanja za subjekte koji uvode sustav.

U cilju uklanjanja ili smanjenja rizika povezanih s korištenjem visokorizičnog UI sustava u obzir se na odgovarajući način uzimaju tehničko znanje, iskustvo, obrazovanje i osposobljavanje koje treba očekivati od subjekta koji uvodi sustav te pretpostavljeni kontekst u kojem se sustav namjerava koristiti.

- 6. Visokorizični UI sustavi testiraju se kako bi se utvrdile najprikladnije i ciljane mjere upravljanja rizikom. Testiranjem se osigurava da visokorizični UI sustavi postojano rade u skladu sa svojom namjenom i da ispunjavaju zahtjeve utvrđene u ovom odjeljku.
- 7. Postupci testiranja mogu uključivati testiranje u stvarnim uvjetima u skladu s člankom 60.

8. Visokorizični UI sustavi testiraju se prema potrebi u bilo kojem trenutku razvojnog procesa, a u svakom slučaju prije stavljanja na tržište ili u upotrebu. Testiranje se provodi u odnosu na prethodno definirane parametre i probabilističke pragove koji su primjereni za namjenu visokorizičnog UI sustava.
9. Pri provedbi sustava upravljanja rizikom predviđenog u stavcima od 1. do 7. dobavljači razmatraju je li vjerojatno da će, s obzirom na njegovu namjenu, visokorizični UI sustav imati nepovoljan utjecaj na osobe mlađe od 18 godina i, prema potrebi, na druge skupine ranjivih osoba.
10. Kad je riječ o dobavljačima visokorizičnih UI sustava na koje se primjenjuju zahtjevi u pogledu unutarnjih procesa upravljanja rizikom na temelju drugih relevantnih odredaba prava Unije, aspekti iz stavaka od 1. do 9. mogu biti dio postupaka upravljanja rizikom uspostavljenih na temelju tog prava ili se kombinirati s tim postupcima.

Članak 10.

Podaci i upravljanje podacima

1. Visokorizični UI sustavi koji upotrebljavaju tehnike s treniranjem UI modelâ s pomoću podataka moraju se razvijati na temelju skupova podataka za treniranje, validaciju i testiranje koji ispunjavaju kriterije kvalitete iz stavaka od 2. do 5. kad god se takvi skupovi podataka upotrebljavaju.

2. Na skupove podataka za treniranje, validaciju i testiranje primjenjuju se prakse upravljanja i rukovanja podacima prikladne za namjenu visokorizičnog UI sustava. Te se prakse ponajprije odnose na:
- (a) relevantne odluke o dizajnu;
 - (b) procese prikupljanja podataka i podrijetlo podataka te, u slučaju osobnih podataka, izvornu svrhu prikupljanja podataka;
 - (c) relevantne postupke obrade za pripremu podataka, kao što su obilježavanje, označivanje, čišćenje, ažuriranje, obogaćivanje i agregiranje;
 - (d) formuliranje pretpostavki, osobito s obzirom na informacije koje bi podaci trebali mjeriti i predstavljati;
 - (e) procjenu raspoloživosti, količine i prikladnosti potrebnih skupova podataka;
 - (f) ispitivanje s obzirom na moguće pristranosti koje bi mogle utjecati na zdravlje i sigurnost osoba, imati negativan utjecaj na temeljna prava ili dovesti do diskriminacije zabranjene pravom Unije, posebno ako izlazni podaci utječu na ulazne podatke za buduće operacije;
 - (g) odgovarajuće mjere za otkrivanje, sprečavanje i ublažavanje mogućih pristranosti utvrđenih u skladu s točkom (f);
 - (h) utvrđivanje relevantnih nedostataka u podacima ili drugih nedostataka koji onemogućuju usklađivanje s ovom Uredbom te načina na koji se ti nedostaci mogu ukloniti.

3. Skupovi podataka za treniranje, validaciju i testiranje moraju biti relevantni, dovoljno reprezentativni te, u najvećoj mogućoj mjeri, bez pogrešaka i potpuni s obzirom na namjenu. Moraju imati odgovarajuća statistička obilježja, među ostalim u odnosu na osobe ili skupine osoba u pogledu kojih se visokorizični UI sustav namjerava koristiti, ako je primjenjivo. Te se karakteristike skupova podataka mogu postići na razini pojedinačnih skupova podataka ili na razini kombinacije skupova podataka.
4. U skupovima podataka moraju se uzeti u obzir, u mjeri u kojoj to iziskuje namjena, karakteristike ili elementi specifični za zemljopisno, kontekstualno, bihevioralno ili radno okruženje u kojem se visokorizični UI sustav namjerava koristiti.
5. U mjeri u kojoj je to nužno u svrhu osiguravanja otkrivanja i ispravljanja pristranosti u vezi s visokorizičnim UI sustavima u skladu sa stavkom 2. točkama (f) i (g) ovog članka, dobavljači takvih sustava mogu iznimno obrađivati posebne kategorije osobnih podataka, podložno odgovarajućim zaštitnim mjerama za temeljna prava i slobode fizičkih osoba. Kako bi se takva obrada provela, uz odredbe utvrđene u uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivi (EU) 2016/680 moraju se ispuniti svi sljedeći uvjeti:
 - (a) otkrivanje i ispravljanje pristranosti ne može se djelotvorno postići obradom drugih podataka, uključujući sintetičke ili anonimizirane podatke;

- (b) posebne kategorije osobnih podataka podliježu tehničkim ograničenjima u pogledu ponovne upotrebe osobnih podataka i najsuvremenijim mjerama sigurnosti i zaštite privatnosti, uključujući pseudonimizaciju;
- (c) posebne kategorije osobnih podataka podliježu mjerama kojima se osigurava da su obrađeni osobni podaci osigurani i zaštićeni, podložno odgovarajućim zaštitnim mjerama, uključujući stroge kontrole i dokumentaciju pristupa, kako bi se izbjegla pogrešna upotreba i osiguralo da pristup tim osobnim podacima imaju samo ovlaštene osobe i uz odgovarajuće obveze u pogledu povjerljivosti;
- (d) posebne kategorije osobnih podataka ne smiju se prenositi, prosljeđivati niti im druge strane smiju na neki drugi način pristupiti;
- (e) posebne kategorije osobnih podataka brišu se nakon ispravljanja pristranosti ili završetka razdoblja čuvanja osobnih podataka, ovisno o tome što nastupi ranije;
- (f) evidencija aktivnosti obrade na temelju uredaba (EU) 2016/679 i (EU) 2018/1725 te Direktive (EU) 2016/680 sadržava razloge zbog kojih je obrada posebnih kategorija osobnih podataka bila nužna za otkrivanje i ispravljanje pristranosti te zbog kojih se taj cilj nije mogao postići obradom drugih podataka.

6. Kad je riječ o razvoju visokorizičnih UI sustava u kojima se ne upotrebljavaju tehnike koje uključuju treniranje UI modelâ, stavci od 2. do 5. primjenjuju se samo na skupove podataka za testiranje.

Članak 11.

Tehnička dokumentacija

1. Tehnička dokumentacija visokorizičnog UI sustava sastavlja se prije njegova stavljanja na tržište ili u upotrebu te se ažurira.

Tehnička dokumentacija sastavlja se tako da se njome dokaže da visokorizični UI sustav ispunjava zahtjeve utvrđene u ovom odjeljku te da se nacionalnim nadležnim tijelima i prijavljenim tijelima na jasan i sveobuhvatan način pruže informacije potrebne za ocjenjivanje usklađenosti UI sustava s tim zahtjevima. Tehnička dokumentacija sadržava barem elemente utvrđene u Prilogu IV. MSP-ovi, uključujući *start-up* poduzeća, mogu elemente tehničke dokumentacije iz Priloga IV. dostaviti na pojednostavnjen način. U tom cilju Komisija utvrđuje pojednostavnjeni obrazac za tehničku dokumentaciju namijenjen potrebama malih poduzeća i mikropoduzeća. Ako MSP, uključujući *start-up* poduzeće, odluči na pojednostavnjen način dostaviti informacije koje se zahtijevaju u Prilogu IV., koristi se obrascem na koji se upućuje u ovom stavku. Prijavljena tijela prihvataju taj obrazac u svrhu ocjenjivanja sukladnosti.

2. Ako se na tržište ili u upotrebu stavlja visokorizični UI sustav povezan s proizvodom koji je obuhvaćen zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., sastavlja se jedinstvena tehnička dokumentacija koja sadržava sve informacije utvrđene u stavku 1., kao i informacije koje se zahtijevaju tim pravnim aktima.

3. Komisija ja ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene, prema potrebi, Priloga IV. kako bi se osiguralo da, s obzirom na tehnički napredak, tehnička dokumentacija sadržava sve informacije potrebne za ocjenjivanje usklađenosti sustava sa zahtjevima utvrđenima u ovom odjeljku.

Članak 12.

Čuvanje evidencije

1. Kod visokorizičnih UI sustava mora biti tehnički omogućeno automatsko evidentiranje događaja („evidencija”) tijekom cijelog životnog ciklusa sustava.
2. Kako bi se osigurala određena razina sljedivosti funkcioniranja visokorizičnog UI sustava koja je u skladu s namjenom sustava, funkcije evidentiranja događaja omogućuju evidentiranje događaja relevantnih za:
 - (a) utvrđivanje situacija koje mogu dovesti do toga da visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1. ili do znatne izmjene;
 - (b) olakšavanje praćenja nakon stavljanja na tržište iz članka 72.; i
 - (c) praćenje rada visokorizičnih UI sustava iz članka 26. stavka 5.
3. Kad je riječ o visokorizičnim UI sustavima iz točke 1. podtočke (a) Priloga III., funkcijama evidentiranja evidentira se najmanje:
 - (a) razdoblje svake upotrebe sustava (datum i vrijeme početka te datum i vrijeme završetka svake upotrebe);

- (b) referentna baza podataka s kojom je sustav usporedio ulazne podatke;
- (c) ulazni podaci za koje je pretragom utvrđena podudarnost;
- (d) identitet fizičkih osoba iz članka 14. stavka 5. koje su sudjelovale u provjeri rezultata.

Članak 13.

Transparentnost i pružanje informacija subjektima koji uvode sustav

1. Visokorizični UI sustavi dizajniraju se i razvijaju na takav način da se osigura da je njihov rad dovoljno transparentan kako bi se subjektima koji uvode sustav omogućilo da tumače izlazne podatke sustava i primjereno ih upotrebljavaju. Osiguravaju se odgovarajuća vrsta i stupanj transparentnosti kako bi se ispunile relevantne obveze dobavljača i subjekta koji uvodi sustav utvrđene u odjeljku 3.
2. Visokorizičnim UI sustavima prilažu se upute za korištenje u odgovarajućem digitalnom ili drugom formatu sa sažetom, potpunom, točnom i jasnim informacijama koje su subjektima koji uvode sustav relevantne, pristupačne i razumljive.
3. Upute za korištenje sadržavaju barem sljedeće informacije:
 - (a) identitet i kontaktne podatke dobavljača i, ako je primjenjivo, njegova ovlaštenog zastupnika;

- (b) karakteristike, sposobnosti i ograničenja učinkovitosti visokorizičnog UI sustava, uključujući:
- i. njegovu namjenu;
 - ii. razinu točnosti, uključujući njezine parametre, te razinu otpornosti i kibernetičke sigurnosti iz članka 15. u odnosu na koju je visokorizični UI sustav testiran i validiran i koja se može očekivati, te sve poznate i predvidljive okolnosti koje mogu utjecati na tu očekivanu razinu točnosti, otpornosti i kibernetičke sigurnosti;
 - iii. sve poznate ili predvidljive okolnosti povezane s korištenjem visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive pogrešne upotrebe koje mogu prouzročiti rizike za zdravlje i sigurnost ili temeljna prava iz članka 9. stavka 2.;
 - iv. ako je primjenjivo, tehničke sposobnosti i karakteristike visokorizičnog UI sustava za pružanje informacija koje su relevantne za objašnjenje njegovih izlaznih podataka;
 - v. prema potrebi, učinkovitost sustava u odnosu na konkretne osobe ili skupine osoba na kojima se sustav namjerava koristiti;
 - vi. prema potrebi, specifikacije ulaznih podataka ili sve ostale relevantne informacije o korištenim skupovima podataka za treniranje, validaciju i testiranje, uzimajući u obzir namjenu visokorizičnog UI sustava;

- vii. ako je primjenjivo, informacije koje subjektima koji uvode sustav omogućuju tumačenje izlaznih podataka visokorizičnog UI sustava i njihovu prikladnu upotrebu;
- (c) eventualne promjene visokorizičnog UI sustava i njegove učinkovitosti koje je dobavljač unaprijed odredio u trenutku početnog ocjenjivanja sukladnosti;
- (d) mjere ljudskog nadzora iz članka 14., uključujući tehničke mjere uvedene kako bi se subjektima koji uvode sustav olakšalo tumačenje izlaznih podataka visokorizičnih UI sustava;
- (e) potrebne računalne i hardverske resurse, očekivani životni ciklus visokorizičnog UI sustava i sve potrebne mjere održavanja i brige, uključujući njihovu učestalost, kako bi se osiguralo pravilno funkcioniranje tog UI sustava, što se odnosi i na softverska ažuriranja;
- (f) prema potrebi, opis mehanizama uključenih u visokorizični UI sustav koji omogućuje subjektima koji uvode sustav da pravilno prikupljaju, pohranjuju i tumače evidenciju u skladu s člankom 12.

Članak 14.

Ljudski nadzor

1. Visokorizični UI sustavi dizajniraju se i razvijaju na takav način, među ostalim s odgovarajućim alatima sučelja čovjek-stroj, da ih fizičke osobe mogu djelotvorno nadzirati tijekom njihove upotrebe.

2. Cilj je ljudskog nadzora spriječiti ili što više smanjiti rizike za zdravlje, sigurnost ili temeljna prava koji se mogu pojaviti tijekom upotrebe visokorizičnog UI sustava u skladu s njegovom namjenom ili u uvjetima razumno predvidljive pogrešne upotrebe, osobito ako takvi rizici i dalje postoje unatoč primjeni drugih zahtjeva utvrđenih u ovom odjeljku.
3. Mjere nadzora razmjerne su rizicima, razini autonomije i kontekstu korištenja visokorizičnog UI sustava, a osiguravaju se barem jednom od sljedećih vrsta mjera:
 - (a) mjerama koje dobavljač utvrđuje i ugrađuje, ako je to tehnički izvedivo, u visokorizični UI sustav prije njegova stavljanja na tržište ili u upotrebu;
 - (b) mjerama koje dobavljač utvrđuje prije stavljanja visokorizičnog UI sustava na tržište ili u upotrebu, a koje su primjerene da ih provodi subjekt koji uvodi sustav.
4. Za potrebe provedbe stavaka 1., 2. i 3. visokorizični UI sustav isporučuje se subjektu koji uvodi sustav na takav način da fizičke osobe kojima je povjeren ljudski nadzor mogu, ako je to potrebno i razmjerno:
 - (a) pravilno razumjeti relevantne kapacitete i ograničenja visokorizičnog UI sustava i biti sposobne na odgovarajući način pratiti njegov rad, među ostalim radi otkrivanja i uklanjanja nepravilnosti, disfunkcija i neočekivanih rezultata;

- (b) biti na oprezu u pogledu moguće tendencije automatskog ili pretjeranog oslanjanja na izlazne podatke visokorizičnog UI sustava („automatizacijska pristranost”), osobito kad je riječ o visokorizičnim UI sustavima koji se upotrebljavaju za davanje informacija ili preporuka na temelju kojih odluke donose fizičke osobe;
- (c) točno protumačiti izlazne podatke visokorizičnog UI sustava, uzimajući u obzir, primjerice, dostupne alate i metode za tumačenje;
- (d) u određenoj situaciji odustati od upotrebe visokorizičnog UI sustava ili na neki drugi način zanemariti, nadjačati ili poništiti izlazni podatak visokorizičnog UI sustava;
- (e) intervenirati u rad visokorizičnog UI sustava ili prekinuti rad sustava pritiskom gumba za zaustavljanje ili sličnim postupkom koji omogućuje sigurno zaustavljanje sustava.

5. Kad je riječ o visokorizičnim UI sustavima iz točke 1. podtočke (a) Priloga III., mjerama iz stavka 3. ovog članka mora se usto osigurati da subjekt koji uvodi sustav ne poduzima nikakve radnje ili odluke na temelju identifikacije proizišle iz sustava ako identifikaciju nisu zasebno provjerile i potvrdile barem dvije fizičke osobe koje imaju potrebne kompetencije, osposobljenost i ovlasti.

Zahtjev da najmanje dvije fizičke osobe moraju provesti zasebnu provjeru ne primjenjuje se na visokorizične UI sustave koji se upotrebljavaju u svrhu kaznenog progona, migracija, nadzora državne granice ili azila ako se u pravu Unije ili nacionalnom pravu primjena tog zahtjeva smatra nerazmjernom.

Članak 15.

Točnost, otpornost i kibernetička sigurnost

1. Visokorizični UI sustavi dizajniraju se i razvijaju tako da postignu odgovarajuću razinu točnosti, otpornosti i kibernetičke sigurnosti te da im je u tim aspektima radni učinak tijekom cijelog životnog ciklusa konstantan.
2. Kako bi se uvažili tehnički aspekti načina mjerenja odgovarajućih razina točnosti i otpornosti iz stavka 1. i ostali relevantni parametri učinkovitosti, Komisija u suradnji s relevantnim dionicima i organizacijama, kao što su tijela za mjeriteljstvo i utvrđivanje referentnih vrijednosti, prema potrebi potiče razvoj referentnih vrijednosti i metodologija mjerenja.
3. Razine točnosti i relevantni parametri točnosti visokorizičnih UI sustava navode se u popratnim uputama za korištenje.
4. Visokorizični UI sustavi moraju biti otporni što je više moguće na greške, kvarove ili nedosljednosti koji se mogu dogoditi unutar sustava ili okruženja u kojem sustav radi, osobito zbog njihove interakcije s fizičkim osobama ili drugim sustavima. U tom se pogledu moraju poduzimati tehničke i organizacijske mjere.

Otpornost visokorizičnih UI sustava može se postići tehničkom redundancijom, što može uključivati pričuvne planove ili sigurnosne planove.

Visokorizični UI sustavi koji nastavljaju učiti nakon stavljanja na tržište ili u upotrebu razvijaju se na takav način da se otkloni ili na najmanju moguću mjeru svede rizik od potencijalno pristranih izlaznih podataka koji utječu na ulazne podatke u budućim operacijama („povratne veze”) te da se osigura da se na takve eventualne povratne veze na odgovarajući način reagira primjerenim mjerama ublažavanja.

5. Visokorizični UI sustavi moraju biti otporni na pokušaje neovlaštenih trećih strana da im izmijene upotrebu, izlazne podatke ili učinkovitost iskorištavanjem slabih točaka sustava.

Tehnička rješenja za osiguravanje kibernetičke sigurnosti visokorizičnih UI sustava moraju biti primjerena relevantnim okolnostima i rizicima.

Tehnička rješenja za prevladavanje specifičnih slabih točaka umjetne inteligencije obuhvaćaju, prema potrebi, mjere za sprečavanje, otkrivanje, odgovor, rješavanje i kontrolu u vezi s napadima čiji je cilj manipuliranje skupom podataka za treniranje („trovanje podataka”) ili prethodno treniranim komponentama koje se upotrebljavaju u treniranju („trovanje modela”), ulaznim podacima osmišljenima kako bi UI model načinio pogrešku („neprijateljski primjeri” ili „zaobilaženje modela”), napadima na povjerljivost ili nedostacima modela.

ODJELJAK 3.
OBVEZE DOBAVLJAČA VISOKORIZIČNIH UI SUSTAVA
I SUBJEKATA KOJI IH UVODE TE DRUGIH STRANA

Članak 16.

Obveze dobavljača visokorizičnih UI sustava

Dobavljači visokorizičnih UI sustava:

- (a) osiguravaju da njihovi visokorizični UI sustavi ispunjavaju zahtjeve utvrđene u odjeljku 2.;
- (b) na visokorizičnom UI sustavu ili, ako to nije moguće, na njegovoj ambalaži ili u njegovoj popratnoj dokumentaciji, ovisno o slučaju, navode svoje ime, registrirano trgovačko ime ili registrirani žig te adresu za kontakt;
- (c) imaju uspostavljen sustav upravljanja kvalitetom koji je u skladu s člankom 17.;
- (d) vode dokumentaciju iz članka 18.;
- (e) čuvaju evidenciju koju automatski generiraju njihovi visokorizični UI sustavi dok su pod njihovom kontrolom, kako je navedeno u članku 19.;
- (f) osiguravaju da visokorizični UI sustav prije stavljanja na tržište ili u upotrebu prođe relevantni postupak ocjenjivanja sukladnosti iz članka 43.;

- (g) sastavljaju EU izjavu o sukladnosti u skladu s člankom 47.;
- (h) stavljaju oznaku CE na visokorizični UI sustav ili, ako to nije moguće, na njegovu ambalažu ili u njegovu popratnu dokumentaciju kako bi se označila sukladnost s ovom Uredbom, u skladu s člankom 48.;
- (i) ispunjavaju obveze registracije iz članka 49. stavka 1.;
- (j) poduzimaju potrebne korektivne mjere i pružaju informacije u skladu s člankom 20.;
- (k) na obrazloženi zahtjev nacionalnog nadležnog tijela dokazuju sukladnost visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2.;
- (l) osiguravaju da visokorizični UI sustav ispunjava zahtjeve u pogledu pristupačnosti u skladu s direktivama (EU) 2016/2102 i (EU) 2019/882.

Članak 17.

Sustav upravljanja kvalitetom

1. Dobavljači visokorizičnih UI sustava uspostavljaju sustav upravljanja kvalitetom kojim se osigurava usklađenost s ovom Uredbom. O tom se sustavu na sustavan i uredan način sastavlja dokumentacija u obliku pisanih politika, postupaka i uputa, a obuhvaća barem sljedeće aspekte:
 - (a) strategiju za usklađenost s propisima, uključujući usklađenost s postupcima ocjenjivanja sukladnosti i postupcima za upravljanje izmjenama visokorizičnog UI sustava;

- (b) tehnike, postupke i sustavne aktivnosti koji se moraju provoditi u dizajnu te kontroli i provjeri dizajna visokorizičnog UI sustava;
- (c) tehnike, postupke i sustavne aktivnosti koji se moraju provoditi u razvoju te kontroli kvalitete i osiguravanju kvalitete visokorizičnog UI sustava;
- (d) postupke ispitivanja, testiranja i validacije koji se moraju provoditi prije, tijekom i poslije razvoja visokorizičnog UI sustava te učestalost kojom se moraju provoditi;
- (e) tehničke specifikacije, uključujući norme, koje se moraju primjenjivati i, ako relevantne usklađene norme nisu u cijelosti primijenjene ili ne obuhvaćaju sve relevantne zahtjeve utvrđene u odjeljku 2., sredstva koja se moraju upotrijebiti kako bi se osigurala usklađenost visokorizičnog UI sustava s tim zahtjevima;
- (f) sustave i postupke za upravljanje podacima, uključujući pribavljanje podataka, prikupljanje podataka, analizu podataka, označivanje podataka, pohranu podataka, filtriranje podataka, rudarenje podataka, agregiranje podataka, zadržavanje podataka i sve druge operacije s podacima koje se obavljaju prije stavljanja visokorizičnih UI sustava na tržište ili u upotrebu i u svrhu tog stavljanja;
- (g) sustav upravljanja rizikom iz članka 9.;
- (h) uspostavu, primjenu i održavanje sustava praćenja nakon stavljanja na tržište u skladu s člankom 72.;

- (i) postupke povezane s prijavljivanjem ozbiljnog incidenta u skladu s člankom 73.;
 - (j) postupke komunikacije s nacionalnim nadležnim tijelima, drugim relevantnim tijelima, uključujući tijela za pružanje ili olakšavanje pristupa podacima, prijavljenim tijelima, drugim operaterima, klijentima ili drugim zainteresiranim stranama;
 - (k) sustave i postupke za čuvanje evidencije o svojoj relevantnoj dokumentaciji i svim relevantnim informacijama;
 - (l) upravljanje resursima, uključujući mjere koje se odnose na sigurnost opskrbe;
 - (m) okvir za odgovornost kojim se utvrđuju odgovornosti uprave i drugog osoblja za sve aspekte navedene u ovom stavku.
2. Aspekti iz stavka 1. provode se razmjerno veličini dobavljačeve organizacije. Dobavljači u svakom slučaju moraju poštovati stupanj strogosti i razinu zaštite koji su potrebni kako bi se osigurala usklađenost njihovih UI sustava s ovom Uredbom.
3. Dobavljači visokorizičnih UI sustava koji podliježu obvezama u pogledu sustavâ upravljanja kvalitetom ili jednakovrijedne funkcije na temelju relevantnog sektorskog prava Unije mogu uključiti aspekte navedene u stavku 1. u sustave upravljanja kvalitetom u skladu s tim pravom.

4. Kad je riječ o dobavljačima koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama, obveza uspostave sustava upravljanja kvalitetom, uz iznimku stavka 1. točaka (g), (h) i (i) ovog članka, smatra se ispunjenom ako se poštuju pravila o unutarnjem upravljanju, aranžmanima ili procesima u skladu s relevantnim pravom Unije o financijskim uslugama. U tom se cilju u obzir uzimaju sve usklađene norme iz članka 40.

Članak 18.

Čuvanje dokumentacije

1. Tijekom razdoblja od deset godina nakon što je visokorizični UI sustav umjetne inteligencije stavljen na tržište ili u upotrebu dobavljač nacionalnim nadležnim tijelima na raspolaganju drži:
- (a) tehničku dokumentaciju iz članka 11.;
 - (b) dokumentaciju o sustavu upravljanja kvalitetom iz članka 17.;
 - (c) dokumentaciju o promjenama koje su odobrila prijavljena tijela, ako je primjenjivo;
 - (d) odluke i druge dokumente koje su izdala prijavljena tijela, ako je primjenjivo;
 - (e) EU izjavu o sukladnosti iz članka 47.

2. Svaka država članica određuje uvjete pod kojima dokumentacija iz stavka 1. ostaje na raspolaganju nacionalnim nadležnim tijelima tijekom razdoblja navedenog u tom stavku u slučaju da dobavljač ili njegov ovlašteni zastupnik s poslovnim nastanom na njezinu državnom području proglasi stečaj ili prestane s radom prije kraja tog razdoblja.
3. Dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama čuvaju tehničku dokumentaciju u sklopu dokumentacije koja se čuva na temelju relevantnog prava Unije o financijskim uslugama.

Članak 19.

Automatski generirana evidencija

1. Dobavljači visokorizičnih UI sustava čuvaju evidenciju iz članka 12. stavka 1. koju automatski generiraju njihovi visokorizični UI sustavi u mjeri u kojoj je takva evidencija pod njihovom kontrolom. Ne dovodeći u pitanje primjenjivo pravo Unije ili nacionalno pravo, evidencija se čuva u razdoblju koje je primjereno namjeni visokorizičnog UI sustava, a najmanje šest mjeseci, osim ako je drukčije predviđeno u primjenjivom pravu Unije ili nacionalnom pravu, a posebno u pravu Unije o zaštiti osobnih podataka.
2. Dobavljači koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama čuvaju evidenciju koju automatski generiraju njihovi visokorizični UI sustavi u sklopu dokumentacije koja se čuva na temelju relevantnog prava o financijskim uslugama.

Članak 20.

Korektivne mjere i obveza obavješćivanja

1. Dobavljači visokorizičnih UI sustava koji smatraju ili imaju razloga smatrati da visokorizični UI sustav koji su stavili na tržište ili u upotrebu nije sukladan s ovom Uredbom odmah poduzimaju potrebne korektivne mjere kako bi, prema potrebi, postigli sukladnost tog sustava s ovom Uredbom, povukli ga, onesposobili ili ga opozvali. O dotičnom visokorizičnom UI sustavu na odgovarajući obavješćuju distributere i, ako je primjenjivo, subjekte koji uvode sustav, ovlaštenog zastupnika i uvoznike.
2. Ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1. i dobavljač sustava sazna za taj rizik, on odmah istražuje uzroke, ako je primjenjivo u suradnji sa subjektom koji uvodi sustav i koji je to prijavio, te obavješćuje tijela za nadzor tržišta koja su nadležna za dotični visokorizični UI i, ako je primjenjivo, prijavljeno tijelo koje je izdalo potvrdu za taj visokorizični UI sustav u skladu s člankom 44., osobito o prirodi neusklađenosti i relevantnim korektivnim mjerama koje su eventualno već poduzete.

Članak 21.

Suradnja s nadležnim tijelima

1. Dobavljači visokorizičnih UI sustava nadležnom tijelu na njegov obrazloženi zahtjev dostavljaju sve informacije i dokumentaciju koji su potrebni za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. na jednom od službenih jezika institucija Unije koji je navela dotična država članica i koji to tijelo može bez poteškoća razumjeti.
2. Na obrazloženi zahtjev nadležnog tijela dobavljači nadležnom tijelu koje je podnijelo zahtjev, ako je primjenjivo, također daju pristup automatski generiranoj evidenciji visokorizičnog UI sustava iz članka 12. stavka 1. u mjeri u kojoj je takva evidencija pod njihovom kontrolom.
3. Sa svim informacijama koje nadležno tijelo pribavi na temelju ovog članka postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 22.

Ovlašteni zastupnici dobavljača visokorizičnih UI sustava

1. Prije stavljanja svojih visokorizičnih UI sustava na tržište Unije dobavljači s poslovnim nastanom u trećim zemljama pisanim ovlaštenjem imenuju ovlaštenog zastupnika s poslovnim nastanom u Uniji.

2. Dobavljač omogućuje svojem ovlaštenom zastupniku da obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača.
3. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača. On na zahtjev dostavlja primjerak ovlaštenja tijelima za nadzor tržišta na jednom od službenih jezika institucije Unije koji je navelo nadležno tijelo. Za potrebe ove Uredbe ovlaštenjem se ovlaštenom zastupniku daje ovlast da obavlja sljedeće zadaće:
 - (a) provjerava jesu li sastavljene EU izjava o sukladnosti iz članka 47. i tehnička dokumentacija iz članka 11. i je li dobavljač proveo odgovarajući postupak ocjenjivanja sukladnosti;
 - (b) nadležnim tijelima te nacionalnim tijelima iz članka 74. stavka 10., tijekom razdoblja od deset godina nakon što je visokorizični UI sustav stavljen na tržište ili u upotrebu, drži na raspolaganju kontaktne podatke dobavljača koji je imenovao ovlaštenog zastupnika, primjerak EU izjave o sukladnosti iz članka 47., tehničku dokumentaciju i, ako je primjenjivo, potvrdu koju je izdalo prijavljeno tijelo;
 - (c) nadležnom tijelu na obrazloženi zahtjev dostavlja sve informacije i dokumentaciju, uključujući one iz točke (b) ovog podstavka, koji su potrebni za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2., što uključuje pristup evidenciji iz članka 12. stavka 1. koju automatski generira visokorizični UI sustav u mjeri u kojoj je takva evidencija pod kontrolom dobavljača;

- (d) na obrazloženi zahtjev surađuje s nadležnim tijelima u svim aktivnostima koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom, posebno kako bi se smanjili i ublažili rizici koje predstavlja visokorizični UI sustav;
- (e) ako je primjenjivo, ispunjava obveze registracije iz članka 49. stavka 1. ili, ako registraciju provodi sam dobavljač, osigurava točnost informacija iz točke 3. odjeljka A Priloga VIII.

Ovlaštenjem se ovlaštenom zastupniku daje ovlast da mu se, uz dobavljača ili umjesto dobavljaču, obraćaju nadležna tijela u vezi sa svim pitanjima povezanim s osiguravanjem usklađenosti s ovom Uredbom.

- 4. Ovlašteni zastupnik ukida ovlaštenje ako smatra ili ima razloga smatrati da dobavljač postupi protivno svojim obvezama na temelju ove Uredbe. U tom slučaju ovlašteni zastupnik o ukidanju ovlaštenja i razlozima za ukidanje odmah obavješćuje relevantno tijelo za nadzor tržišta i, ako je primjenjivo, relevantno prijavljeno tijelo.

Članak 23.

Obveze uvoznika

- 1. Prije stavljanja visokorizičnog UI sustava na tržište uvoznici osiguravaju da je sustav sukladan s ovom Uredbom tako da provjere je li:
 - (a) dobavljač visokorizičnog UI sustava proveo relevantni postupak ocjenjivanja sukladnosti iz članka 43.;

- (b) dobavljač sastavio tehničku dokumentaciju u skladu s člankom 11. i Prilogom IV.;
 - (c) sustav označen oznakom CE te jesu li mu priložene EU izjava o sukladnosti iz članka 47. i upute za korištenje;
 - (d) dobavljač imenovao ovlaštenog zastupnika u skladu s člankom 22. stavkom 1.
2. Ako uvoznik ima dovoljno razloga smatrati da visokorizični UI sustav nije sukladan s ovom Uredbom, da je krivotvoren ili da mu je priložena krivotvorena dokumentacija, ne stavlja taj sustav na tržište dok on ne postane sukladan s ovom Uredbom.
- Ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1., uvoznik o tome obavješćuje dobavljača sustava, ovlaštene zastupnike i tijela za nadzor tržišta.
3. Uvoznici navode svoje ime, registrirano trgovačko ime ili registrirani žig i adresu za kontakt na visokorizičnom UI sustavu i na njegovoj ambalaži ili u njegovoj popratnoj dokumentaciji, ako je primjenjivo.
4. Dok je visokorizični UI sustav pod njihovom odgovornošću uvoznici osiguravaju da uvjeti skladištenja ili prijevoza, ako je primjenjivo, ne ugrožavaju njegovu usklađenost sa zahtjevima utvrđenima u odjeljku 2.

5. Uvoznici tijekom razdoblja od deset godina nakon što je visokorizični UI sustav stavljen na tržište ili u upotrebu čuvaju primjerak potvrde koju je izdalo prijavljeno tijelo, ako je primjenjivo, uputa za korištenje i EU izjave o sukladnosti iz članka 47.
6. Uvoznici relevantnim nadležnim tijelima na obrazloženi zahtjev dostavljaju sve informacije i dokumentaciju, uključujući informacije i dokumentaciju navedene u stavku 5., koji su potrebni za dokazivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. na jeziku koji ta tijela mogu bez poteškoća razumjeti. U tu svrhu također osiguravaju da se tim tijelima na raspolaganje može staviti tehnička dokumentacija.
7. Uvoznici surađuju s relevantnim nadležnim tijelima u svim mjerama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom koji uvoznici stavljaju na tržište, posebno kako bi se smanjili i ublažili rizici koje on predstavlja.

Članak 24.

Obveze distributerâ

1. Prije stavljanja visokorizičnog UI sustava na raspolaganje na tržištu distributeri provjeravaju ima li on potrebnu oznaku CE, jesu li mu priloženi primjerak EU izjave o sukladnosti iz članka 47. i upute za korištenje te jesu li dobavljač i uvoznik tog sustava, ovisno o slučaju, ispunili svoje obveze utvrđene u članku 16. točkama (b) i (c) i članku 23. stavku 3.

2. Ako distributer na temelju informacija kojima raspolaže smatra ili ima razloga smatrati da visokorizični UI sustav nije sukladan sa zahtjevima utvrđenima u odjeljku 2., ne stavlja visokorizični UI sustav na tržište dok sustav ne postane sukladan s tim zahtjevima. Osim toga, ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1., distributer o tome obavješćuje dobavljača ili uvoznika tog sustava, ovisno o slučaju.
3. Dok je visokorizični UI sustav pod njihovom odgovornošću, distributeri osiguravaju da uvjeti skladištenja ili prijevoza, ako je primjenjivo, ne ugrožavaju njegovu usklađenost sa zahtjevima utvrđenima u odjeljku 2.
4. Ako distributer na temelju informacija kojima raspolaže smatra ili ima razloga smatrati da visokorizični UI sustav koji je stavio na raspolaganje na tržištu nije sukladan sa zahtjevima utvrđenima u odjeljku 2., poduzima korektivne mjere potrebne kako bi postigao sukladnost dotičnog sustava s tim zahtjevima, povukao ga ili opozvao ili, osigurava da te korektivne mjere poduzme, prema potrebi, dobavljač, uvoznik ili drugi relevantni operater. Ako visokorizični UI sustav predstavlja rizik u smislu članka 79. stavka 1., distributer o tome odmah obavješćuje dobavljača ili uvoznika sustava i tijela nadležna za dotični visokorizični UI sustav, navodeći pojedinosti, osobito o neusklađenosti i poduzetim korektivnim mjerama.

5. Distributeri visokorizičnog UI sustava relevantnom nadležnom tijelu na obrazloženi zahtjev tog tijela dostavljaju sve informacije i dokumentaciju o svim njihovim mjerama na temelju stavaka od 1. do 4. koje su potrebne za dokazivanje sukladnosti tog sustava sa zahtjevima utvrđenima u odjeljku 2.
6. Distributeri surađuju s relevantnim nadležnim tijelima u svim mjerama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom koji su distributeri stavili na raspolaganje na tržištu, posebno kako bi se smanjili ili ublažili rizici koje on predstavlja.

Članak 25.

Odgovornosti duž vrijednosnog lanca umjetne inteligencije

1. Svi distributeri, uvoznici, subjekti koji uvode sustav ili ostale treće strane smatraju se dobavljačima visokorizičnog UI sustava za potrebe ove Uredbe i podliježu obvezama dobavljača iz članka 16. u bilo kojoj od sljedećih okolnosti:
 - (a) ako stave svoje ime ili žig na visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu, ne dovodeći u pitanje ugovorne aranžmane u kojima je utvrđena drukčija raspodjela obveza;
 - (b) ako znatno izmijene visokorizični UI sustav koji je već stavljen na tržište ili u upotrebu i to na takav način da i dalje ostane visokorizični UI sustav na temelju članka 6.;

- (c) ako izmijene namjenu UI sustava, uključujući UI sustav opće namjene, koji nije klasificiran kao visokorizičan i već je stavljen na tržište ili u upotrebu i to na takav način da dotični UI sustav postane visokorizični UI sustav u skladu s člankom 6.;
2. Ako nastupe okolnosti iz stavka 1., dobavljač koji je prvobitno stavio UI sustav na tržište ili u upotrebu više se ne smatra dobavljačem tog konkretnog UI sustava za potrebe ove Uredbe. Taj početni dobavljač blisko surađuje s novim dobavljačima te stavlja na raspolaganje potrebne informacije i pruža razumno očekivani tehnički pristup i drugu pomoć koji su potrebni za ispunjavanje obveza utvrđenih u ovoj Uredbi, posebno u pogledu poštovanja ocjenjivanja sukladnosti visokorizičnih UI sustava. Ovaj se stavak ne primjenjuje u slučajevima u kojima je početni dobavljač jasno naveo da se njegov UI sustav ne smije promijeniti u visokorizični UI sustav i stoga nije obuhvaćen obvezom predaje dokumentacije.
3. Kad je riječ o visokorizičnim UI sustavima koji su sigurnosna komponenta proizvoda obuhvaćenih zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., proizvođač proizvoda smatra se dobavljačem visokorizičnog UI sustava i podliježe obvezama iz članka 16. u bilo kojoj od sljedećih okolnosti:
- (a) visokorizični UI sustav stavljen je na tržište zajedno s dotičnim proizvodom pod imenom ili žigom proizvođača proizvoda;
 - (b) visokorizični UI sustav stavljen je u upotrebu pod imenom ili žigom proizvođača proizvoda nakon što je proizvod stavljen na tržište.

4. Dobavljač visokorizičnog UI sustava i treća strana koja isporučuje UI sustav, alate, usluge, komponente ili procese koji se upotrebljavaju u visokorizičnom UI sustavu ili su u njega integrirani, pisanim dogovorom utvrđuju informacije, mogućnosti, tehnički pristup i drugu pomoć na temelju općepriznatih najnovijih dostignuća koji su potrebni kako bi dobavljač visokorizičnog UI sustava mogao u potpunosti ispuniti obveze utvrđene u ovoj Uredbi. Ovaj se stavak ne primjenjuje na treće strane koje stavljaju na raspolaganje javnosti alate, usluge, procese ili komponente, osim UI modelâ opće namjene, na temelju besplatne licencije za softver otvorenog koda.

Ured za umjetnu inteligenciju može razviti i preporučiti dobrovoljne modele uvjeta za ugovore između dobavljača visokorizičnih UI sustava i trećih strana koji isporučuju alate, usluge, komponente ili procese koji se upotrebljavaju u visokorizičnim UI sustavima ili su u njih integrirani. Pri izradi tih dobrovoljnih modela uvjeta Ured za umjetnu inteligenciju uzima u obzir moguće ugovorne zahtjeve primjenjive u određenim sektorima ili poslovnim slučajevima. Dobrovoljni modeli uvjeta objavljuju se i besplatno su dostupni u lako upotrebljivom elektroničkom obliku.

5. Stavcima 2. i 3. ne dovodi se u pitanje potreba za poštovanjem i zaštitom prava intelektualnog vlasništva, povjerljivih poslovnih informacija i poslovnih tajni u skladu s pravom Unije i nacionalnim pravom.

Članak 26.

Obveze subjekata koji uvode visokorizične UI sustave

1. Subjekti koji uvode visokorizične UI sustave poduzimaju odgovarajuće tehničke i organizacijske mjere kako bi osigurali da upotrebljavaju takve sustave u skladu s uputama za korištenje priloženima sustavima na temelju stavaka 3. i 6.

2. Subjekti koji uvode sustav dodjeljuju zadaću ljudskog nadzora fizičkim osobama koje imaju potrebne kompetencije, osposobljenost i ovlasti, te im pružaju potrebnu potporu.
3. Obvezama utvrđenima u stavcima 1. i 2. ne dovode se u pitanje druge obveze subjekta koji uvodi sustav na temelju prava Unije ili nacionalnog prava ni sloboda subjekta koji uvodi sustav da organizira svoje resurse i aktivnosti u svrhu provedbe mjera ljudskog nadzora koje je naveo dobavljač.
4. Ne dovodeći u pitanje stavke 1. i 2., subjekt koji uvodi sustav osigurava, u mjeri u kojoj ima kontrolu nad ulaznim podacima, da su ulazni podaci relevantni i dovoljno reprezentativni s obzirom na namjenu visokorizičnog UI sustava.
5. Subjekti koji uvode sustav prate rad visokorizičnog UI sustava u skladu s uputama za korištenje i prema potrebi obavješćuju dobavljače u skladu s člankom 72. Ako subjekti koji uvode sustav imaju razloga smatrati da korištenje visokorizičnog UI sustava u skladu s uputama može dovesti do toga da UI sustav predstavlja rizik u smislu članka 79. stavka 1., o tome bez nepotrebne odgode obavješćuju dobavljača ili distributera i relevantno tijelo za nadzor tržišta te suspendiraju korištenje tog sustava. Ako subjekti koji uvode sustav utvrde ozbiljan incident, o tom incidentu odmah obavješćuju prvo dobavljača, a zatim uvoznika ili distributera i relevantna tijela za nadzor tržišta. Ako subjekt koji uvodi sustav ne može stupiti u kontakt s dobavljačem, članak 73. primjenjuje se *mutatis mutandis*. Ova obveza ne obuhvaća osjetljive operativne podatke subjekata koji uvode UI sustave koji su tijela kaznenog progona.

Kad je riječ o subjektima koji uvode sustav, a koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih postupaka na temelju prava Unije o financijskim uslugama, obveza praćenja utvrđena u prvom podstavku smatra se ispunjenom ako se poštuju pravila o aranžmanima, procesima i mehanizmima unutarnjeg upravljanja na temelju relevantnog prava o financijskim uslugama.

6. Subjekti koji uvode visokorizične UI sustave čuvaju evidenciju koju automatski generira taj visokorizični UI sustav u mjeri u kojoj je takva evidencija pod njihovom kontrolom, tijekom razdoblja koje je primjereno namjeni visokorizičnog UI sustava, a najmanje šest mjeseci, osim ako je drukčije predviđeno u primjenjivom pravu Unije ili nacionalnom pravu, a posebno u pravu Unije o zaštiti osobnih podataka.

Subjekti koji uvode sustav, a koji su financijske institucije na koje se primjenjuju zahtjevi u pogledu njihova unutarnjeg upravljanja, njihovih aranžmana ili njihovih procesa na temelju prava Unije o financijskim uslugama čuvaju evidenciju u sklopu dokumentacije koja se čuva na temelju relevantnog prava Unije o financijskim uslugama.

7. Prije stavljanja u upotrebu ili korištenja visokorizičnog UI sustava na radnom mjestu subjekti koji uvode visokorizični UI sustav, a koji su poslodavci, obavješćuju predstavnike radnika i radnike na koje se to odnosi da će podlijezati upotrebi visokorizičnog UI sustava. Te se informacije pružaju, ako je primjenjivo, u skladu s pravilima i postupcima utvrđenima u pravu Unije i nacionalnom pravu te praksom o informiranju radnika i njihovih predstavnika.

8. Subjekti koji uvode visokorizične UI sustave koji su javna tijela ili institucije, tijela, uredi ili agencije Unije moraju ispunjavati obveze registracije iz članka 49. Ako takvi subjekti koji uvode sustav utvrde da visokorizični UI sustav koji namjeravaju upotrebljavati nije registriran u bazi podataka EU-a iz članka 71., taj sustav ne upotrebljavaju i o tome obavješćuju dobavljača ili distributera.
9. Ako je primjenjivo, subjekti koji uvode visokorizične UI sustave služe se informacijama iz članka 13. ove Uredbe da bi ispunili svoju obvezu provedbe procjene učinka na zaštitu podataka iz članka 35. Uredbe (EU) 2016/679 ili članka 27. Direktive (EU) 2016/680.
10. Ne dovodeći u pitanje Direktivu (EU) 2016/680, u okviru istrage radi ciljane potrage za osobom osumnjičenom ili osuđenom za počinjenje kaznenog djela, subjekt koji uvodi visokorizični UI sustav za naknadnu daljinsku biometrijsku identifikaciju od pravosudnog ili upravnog tijela čija je odluka obvezujuća i podliježe sudskom preispitivanju traži, *ex ante* ili bez nepotrebne odgode, a najkasnije u roku od 48 sati odobrenje za upotrebu tog sustava osim ako se on upotrebljava za početnu identifikaciju potencijalnog osumnjičenika na temelju objektivnih i provjerljivih činjenica izravno povezanih s kaznenim djelom. Svaka upotreba mora biti ograničena na ono što je nužno za istragu određenog kaznenog djela.

Ako je odobrenje zatraženo na temelju prvog podstavka odbijeno, upotreba sustava za naknadnu daljinsku biometrijsku identifikaciju povezanog s tim zatraženim odobrenjem smjesta se zaustavlja te se brišu osobni podaci povezani s upotrebom visokorizičnog UI sustava za koji je zatraženo odobrenje.

Takav visokorizični UI sustav za naknadnu daljinsku biometrijsku identifikaciju ni u kojem se slučaju ne smije upotrebljavati u svrhu kaznenog progona na neciljani način, bez ikakve poveznice s kaznenim djelom, kaznenim postupkom, stvarnom i prisutnom ili stvarnom i predvidljivom prijetnjom kaznenog djela ili potragom za određenom nestalom osobom. Mora se osigurati da tijela kaznenog progona ne mogu donositi odluke koje proizvode negativan pravni učinak na osobu isključivo na temelju izlaznih podataka takvih sustava za naknadnu daljinsku biometrijsku identifikaciju.

Ovim se stavkom ne dovode u pitanje članak 9. Uredbe (EU) 2016/679 i članak 10. Direktive (EU) 2016/680 kad je riječ o obradi biometrijskih podataka.

Neovisno o namjeni ili subjektu koji uvodi sustav, svaka upotreba takvih visokorizičnih UI sustava dokumentira se u relevantnom policijskom spisu i na zahtjev se stavlja na raspolaganje relevantnom tijelu za nadzor tržišta i nacionalnom tijelu za zaštitu podataka, isključujući otkrivanje osjetljivih operativnih podataka povezanih s kaznenim progonom. Ovim se podstavkom ne dovode u pitanje ovlasti dodijeljene nadzornim tijelima Direktivom (EU) 2016/680.

Subjekti koji uvode sustav podnose godišnja izvješća relevantnim tijelima za nadzor tržišta i nacionalnim tijelima za zaštitu podataka o svojoj upotrebi sustavâ za naknadnu daljinsku biometrijsku identifikaciju, isključujući otkrivanje osjetljivih operativnih podataka povezanih s kaznenim progonom. Izvješća mogu biti skupna kako bi obuhvatila više od jednog uvođenja.

Države članice mogu, u skladu s pravom Unije, uvesti restriktivnije propise o upotrebi sustavâ za naknadnu daljinsku biometrijsku identifikaciju.

11. Ne dovodeći u pitanje članak 50. ove Uredbe, subjekti koji uvode visokorizične UI sustave iz Priloga III. koji donose odluke ili pomažu u donošenju odluka povezanih s fizičkim osobama obavješćuju fizičke osobe o tome da podliježu upotrebi visokorizičnog UI sustava. Na visokorizične UI sustave koji se upotrebljavaju u svrhu kaznenog progona primjenjuje se članak 13. Direktive (EU) 2016/680.
12. Subjekti koji uvode sustav surađuju s relevantnim nadležnim tijelima u svim mjerama koje ta tijela poduzimaju u vezi s visokorizičnim UI sustavom radi provedbe ove Uredbe.

Članak 27.

Procjena učinka visokorizičnih UI sustava na temeljna prava

1. Prije uvođenja visokorizičnog UI sustava iz članka 6. stavka 2., uz iznimku visokorizičnih UI sustava namijenjenih za upotrebu u području navedenom u točki 2. Priloga III., subjekti koji uvode sustav koji su javnopravna tijela ili su privatni subjekti koji pružaju javne usluge i subjekti koji uvode visokorizične UI sustave iz točke 5. podtočaka (b) i (c) Priloga III. provode procjenu učinka koji upotreba takvog sustava može imati na temeljna prava. U tu svrhu subjekti koji uvode sustav provode procjenu koja sadržava:
- (a) opis procesa subjekta koji uvodi sustav u kojima će se visokorizični UI sustav upotrebljavati u skladu sa svojom namjenom;
 - (b) opis razdoblja i učestalosti namjeravane upotrebe svakog visokorizičnog UI sustava;

- (c) kategorije fizičkih osoba i skupina na koje će vjerojatno utjecati upotreba sustava u konkretnom kontekstu;
- (d) specifične rizike od štete koji će vjerojatno utjecati na kategorije fizičkih osoba ili skupine osoba identificirane u skladu s točkom (c) ovog stavka, uzimajući u obzir informacije koje je dostavio dobavljač u skladu s člankom 13.;
- (e) opis provedbe mjera ljudskog nadzora u skladu s uputama za korištenje;
- (f) mjere koje se moraju poduzeti u slučaju materijalizacije tih rizika, uključujući aranžmane za unutarnje upravljanje i mehanizme za podnošenje pritužbi.

2. Obveza utvrđene u stavku 1. primjenjuje se na prvu upotrebu visokorizičnog UI sustava. Subjekt koji uvodi sustav može se u sličnim slučajevima osloniti na prethodno provedene procjene učinka na temeljna prava ili postojeću procjenu učinka koju je proveo dobavljač. Ako tijekom upotrebe visokorizičnog UI sustava subjekt koji uvodi sustav smatra da se neki od elemenata iz stavka 1. promijenio ili da nije ažuriran, subjekt koji uvodi sustav poduzima potrebne korake za ažuriranje informacija.
3. Nakon provedbe procjene iz stavka 1. ovog članka subjekt koji uvodi sustav obavješćuje tijelo za nadzor tržišta o njezinim rezultatima, podnošenjem ispunjenog predloška iz stavka 5. ovog članka u okviru obavijesti. U slučaju iz članka 46. stavka 1. subjekti koji uvode sustav mogu biti izuzeti od te obveze obavješćivanja.

4. Ako je bilo koja od obveza utvrđenih u ovom članku već ispunjena procjenom učinka na zaštitu podataka provedenom na temelju članka 35. Uredbe (EU) 2016/679 ili članka 27. Direktive (EU) 2016/680, procjena učinka na temeljna prava iz stavka 1. ovog članka dopunjuje tu procjenu učinka na zaštitu podataka.
5. Ured za umjetnu inteligenciju izrađuje predložak upitnika, među ostalim s pomoću automatiziranog alata, kako bi se subjektima koji uvode sustav olakšalo da na pojednostavnjen način ispune svoje obveze iz ovog članka.

ODJELJAK 4.

TIJELA KOJA PROVODE PRIJAVLJIVANJE I PRIJAVLJENA TIJELA

Članak 28.

Tijela koja provode prijavljivanje

1. Svaka država članica imenuje ili osniva barem jedno tijelo koje provodi prijavljivanje, koje je odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, prijavljivanje i praćenje tijela za ocjenjivanje sukladnosti. Te postupke u suradnji razvijaju tijela koja provode prijavljivanje iz svih država članica.
2. Države članice mogu odlučiti da ocjenjivanje i praćenje iz stavka 1. provodi nacionalno akreditacijsko tijelo u smislu Uredbe (EZ) br. 765/2008 i u skladu s tom uredbom.

3. Tijela koja provode prijavljivanje osnivaju se, organiziraju i rade na takav način da ne dolazi do sukoba interesa s tijelima za ocjenjivanje sukladnosti te da su zajamčene objektivnost i nepristranost njihovih aktivnosti.
4. Tijela koja provode prijavljivanje organizirana su na takav način da odluke povezane s prijavljivanjem tijela za ocjenjivanje sukladnosti donose nadležne osobe različite od osoba koje su provele ocjenjivanje tih tijela.
5. Tijela koja provode prijavljivanje ne smiju nuditi obavljanje aktivnosti niti smiju obavljati aktivnosti koje obavljaju tijela za ocjenjivanje sukladnosti, kao ni usluge savjetovanja na tržišnoj ili konkurentskoj osnovi.
6. Tijela koja provode prijavljivanje u skladu s člankom 78. štite povjerljivost informacija koje su pribavila.
7. Tijela koja provode prijavljivanje moraju imati adekvatan broj članova stručnog osoblja za propisno obavljanje svojih zadaća. Stručno osoblje mora imati, ako je primjenjivo, potrebno stručno znanje za svoju funkciju u područjima kao što su informacijske tehnologije, umjetna inteligencija i pravo, uključujući nadzor temeljnih prava.

Članak 29.

Zahtjev tijela za ocjenjivanje sukladnosti za prijavljivanje

1. Tijela za ocjenjivanje sukladnosti podnose zahtjev za prijavljivanje tijelu koje provodi prijavljivanje u državi članici u kojoj imaju poslovni nastan.

2. Zahtjevu za prijavljivanje prilaže se opis aktivnosti ocjenjivanja sukladnosti, jednog ili više modula za ocjenjivanje sukladnosti i vrsta UI sustava za koje tijelo za ocjenjivanje sukladnosti tvrdi da je nadležno te potvrda o akreditaciji, ako postoji, koju je izdalo nacionalno akreditacijsko tijelo i kojom se potvrđuje da tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve utvrđene u članku 31.

Dodaju se svi valjani dokumenti koji se odnose na postojeća imenovanja, na temelju drugog zakonodavstva Unije o usklađivanju, prijavljenog tijela koje podnosi zahtjev.

3. Ako dotično tijelo za ocjenjivanje sukladnosti ne može predočiti potvrdu o akreditaciji, tijelu koje provodi prijavljivanje dostavlja sve dokumente potrebne za provjeru, priznavanje i redovito praćenje njegova ispunjavanja zahtjeva utvrđenih u članku 31.
4. Kad je riječ o prijavljenim tijelima koja su imenovana na temelju drugog zakonodavstva Unije o usklađivanju, svi dokumenti i potvrde povezani s tim imenovanjima mogu se, prema potrebi, upotrijebiti u postupku njihova imenovanja na temelju ove Uredbe. Prijavljeno tijelo ažurira dokumentaciju iz stavaka 2. i 3. ovog članka u slučaju bilo kakvih relevantnih promjena kako bi tijelu odgovornom za prijavljena tijela omogućilo da prati i provjerava kontinuirano ispunjavanje svih zahtjeva utvrđenih u članku 31.

Članak 30.

Postupak prijavljivanja

1. Tijela koja provode prijavljivanje mogu prijaviti samo tijela za ocjenjivanje sukladnosti koja ispunjavaju zahtjeve utvrđene u članku 31.
2. Tijela koja provode prijavljivanje pomoću alata za elektroničko prijavljivanje koji je razvila i kojim upravlja Komisija dostavljaju prijavu Komisiji i drugim državama članicama o svakom tijelu za ocjenjivanje sukladnosti iz stavka 1.
3. Prijavljivanje iz stavka 2. ovog članka obuhvaća sve pojedinosti o aktivnostima ocjenjivanja sukladnosti, jednom ili više modula za ocjenjivanje sukladnosti, vrstama dotičnih UI sustava te relevantnu potvrdu o stručnosti. Ako se prijavljivanje ne temelji na potvrdi o akreditaciji iz članka 29. stavka 2., tijelo koje provodi prijavljivanje dostavlja Komisiji i drugim državama članicama pisane dokaze kojima se potvrđuju stručnost tijela za ocjenjivanje sukladnosti i aranžmani koji su uspostavljeni kako bi se osiguralo da će se to tijelo redovito pratiti i da će nastaviti ispunjavati zahtjeve utvrđene u članku 31.
4. Dotično tijelo za ocjenjivanje sukladnosti može obavljati aktivnosti prijavljenog tijela samo ako Komisija ili druge države članice ne podnesu prigovor u roku od dva tjedna od prijavljivanja koje je izvršilo tijelo koje provodi prijavljivanje ako prijava uključuje potvrdu o akreditaciji iz članka 29. stavka 2. odnosno u roku od dva mjeseca od prijavljivanja koje je izvršilo tijelo koje provodi prijavljivanje ako prijava uključuje pisane dokaze iz članka 29. stavka 3.

5. Ako se podnesu prigovori, Komisija bez odgode započinje savjetovanja s relevantnim državama članicama i tijelom za ocjenjivanje sukladnosti. S obzirom na savjetovanja Komisija odlučuje je li odobrenje opravdano. Komisija svoju odluku upućuje dotičnoj državi članici i relevantnom tijelu za ocjenjivanje sukladnosti.

Članak 31.

Zahtjevi koji se odnose na prijavljena tijela

1. Prijavljeno tijelo osniva se na temelju nacionalnog prava države članice i ima pravnu osobnost.
2. Prijavljena tijela moraju ispunjavati organizacijske zahtjeve i zahtjeve koji se odnose na upravljanje kvalitetom, resurse i procese koji su potrebni za obavljanje njihovih zadaća, kao i odgovarajuće zahtjeve u pogledu kibernetičke sigurnosti.
3. Organizacijskom strukturom, podjelom odgovornosti, linijama izvješćivanja i radom prijavljenih tijela osigurava se povjerenje u njihovu učinkovitost i u rezultate aktivnosti ocjenjivanja sukladnosti koje ona provode.
4. Prijavljena tijela moraju biti neovisna o dobavljaču visokorizičnog UI sustava u vezi s kojim provode aktivnosti ocjenjivanja sukladnosti. Prijavljena tijela ujedno moraju biti neovisna o svim ostalim operaterima koji imaju gospodarski interes u visokorizičnim UI sustavima koji se ocjenjuju, kao i o svim konkurentima dobavljača. Time se ne sprečava upotreba ocijenjenih visokorizičnih UI sustava koji su potrebni za rad tijela za ocjenjivanje sukladnosti ni upotreba takvih visokorizičnih UI sustava za osobne potrebe.

5. Tijelo koje ocjenjuje sukladnost, njegovo najviše rukovodstvo i osoblje odgovorno za provedbu zadaća ocjenjivanja sukladnosti ne smiju biti izravno uključeni u dizajn, razvoj, stavljanje na tržište ili upotrebu visokorizičnih UI sustava niti smiju zastupati strane uključene u te aktivnosti. Oni ne smiju sudjelovati u aktivnostima koje bi mogle dovesti u pitanje njihovu neovisnost prosudbe ili njihov integritet u vezi s aktivnostima ocjenjivanja sukladnosti za koje su prijavljeni. To se osobito odnosi na usluge savjetovanja.
6. Prijavljena tijela organizirana su i rade na način kojim se jamče neovisnost, objektivnost i nepristranost njihovih aktivnosti. Prijavljena tijela dokumentiraju i primjenjuju strukturu i postupke za očuvanje nepristranosti te za promicanje i primjenu načelâ nepristranosti u cijeloj svojoj organizaciji, među svojim osobljem i u svojim aktivnostima ocjenjivanja.
7. Prijavljena tijela moraju imati uspostavljene dokumentirane postupke kojima se osigurava da njihovo osoblje, odbori, podružnice, podugovaratelji i sva povezana tijela ili osoblje vanjskih tijela u skladu s člankom 78. poštuju povjerljivost informacija koje prime tijekom obavljanja aktivnosti ocjenjivanja sukladnosti, osim ako se otkrivanje tih informacija zahtijeva zakonom. Osoblje prijavljenih tijela obvezno je čuvati profesionalnu tajnu u pogledu svih informacija koje pribavi tijekom obavljanja svojih zadaća na temelju ove Uredbe, osim u odnosu na tijela koja provode prijavljivanje u državi članici u kojoj prijavljena tijela obavljaju svoje aktivnosti.

8. Prijavljena tijela moraju imati uspostavljene postupke za obavljanje aktivnosti kojima se propisno uzimaju u obzir veličina dobavljača, sektor u kojem on posluje, njegova struktura i stupanj složenosti dotičnog UI sustava.
9. Prijavljena tijela sklapaju odgovarajuće osiguranje od odgovornosti za svoje aktivnosti ocjenjivanja sukladnosti, osim ako u skladu s nacionalnim pravom odgovornost preuzima država članica u kojoj imaju poslovni nastan ili je ta država članica sama izravno odgovorna za ocjenjivanje sukladnosti.
10. Prijavljena tijela moraju biti sposobna provoditi sve svoje zadaće na temelju ove Uredbe s najvećom razinom profesionalnog integriteta i potrebnim kompetencijama u određenom području, bez obzira na to provode li te zadaće sama prijavljena tijela ili se one provode u njihovo ime i pod njihovom odgovornošću.
11. Prijavljena tijela moraju imati dostatne unutarnje kompetencije da bi mogla djelotvorno evaluirati zadaće koje u njihovo ime obavljaju vanjske strane. Prijavljeno tijelo mora kontinuirano imati dovoljan broj članova administrativnog, tehničkog, pravnog i znanstvenog osoblja koji posjeduju iskustvo i znanje u vezi s relevantnim vrstama UI sustava, podacima i obradom podataka te u vezi sa zahtjevima utvrđenima u odjeljku 2.
12. Prijavljena tijela sudjeluju u koordinacijskim aktivnostima iz članka 38. Osim toga, izravno sudjeluju ili imaju predstavnika u europskim organizacijama za normizaciju, ili osiguravaju da su upoznata s relevantnim normama i prate razvoj zbivanja.

Članak 32.

Pretpostavka sukladnosti sa zahtjevima koji se odnose na prijavljena tijela

Ako tijelo za ocjenjivanje sukladnosti dokaže svoju sukladnost s kriterijima utvrđenima u relevantnim usklađenim normama ili njihovim dijelovima, na koje su upućivanja objavljena u *Službenom listu Europske unije*, pretpostavlja se da ispunjava zahtjeve utvrđene u članku 31. u mjeri u kojoj primjenjive usklađene norme obuhvaćaju te zahtjeve.

Članak 33.

Podružnice prijavljenih tijela i podugovaranje

1. Ako prijavljeno tijelo određene zadaće povezane s ocjenjivanjem sukladnosti povjeri podugovarateljima ili ih prenese podružnici, ono osigurava da podugovaratelj ili podružnica ispunjava zahtjeve utvrđene u članku 31. te o tome obavješćuje tijelo koje provodi prijavljivanje.
2. Prijavljena tijela preuzimaju punu odgovornost za svoje zadaće koje obavljaju podugovaratelji ili podružnice.
3. Aktivnosti se samo uz suglasnost dobavljača smiju povjeriti podugovaratelju odnosno smije ih provoditi podružnica. Prijavljena tijela objavljuju popis svojih podružnica.
4. Relevantni dokumenti koji se odnose na ocjenjivanje kvalifikacija podugovaratelja ili podružnica i rada koji su oni obavili na temelju ove Uredbe stavljaju se na raspolaganje tijelu koje provodi prijavljivanje tijekom razdoblja od pet godina od datuma okončanja podugovaranja.

Članak 34.

Operativne obveze prijavljenih tijela

1. Prijavljena tijela provjeravaju sukladnost visokorizičnih UI sustava u skladu s postupcima ocjenjivanja sukladnosti utvrđenima u članku 43.
2. Prijavljena tijela pri obavljanju svojih aktivnosti izbjegavaju nepotrebno opterećenje za dobavljače i uzimaju u obzir veličinu dobavljača, sektor u kojem posluje, njegovu strukturu i stupanj složenosti dotičnog visokorizičnog UI sustava, posebno kako bi se na najmanju moguću mjeru sveli administrativno opterećenje i troškovi usklađivanja za mikropoduzeća i mala poduzeća u smislu Preporuke 2003/361/EZ. Prijavljeno tijelo ipak poštuje stupanj strogosti i razinu zaštite koji su potrebni kako bi visokorizični UI sustav ispunjavao zahtjeve ove Uredbe.
3. Prijavljena tijela tijelu koje provodi prijavljivanje iz članka 28. stavljaju na raspolaganje i na zahtjev dostavljaju svu relevantnu dokumentaciju, uključujući dokumentaciju dobavljača, kako bi to tijelo moglo provoditi svoje aktivnosti ocjenjivanja, imenovanja, prijavljivanja i praćenja te kako bi se olakšalo ocjenjivanje opisano u ovom odjeljku.

Članak 35.

Identifikacijski brojevi i popisi prijavljenih tijela

1. Komisija svakom prijavljenom tijelu dodjeljuje jedinstveni identifikacijski broj, čak i ako je tijelo prijavljeno na temelju više od jednog akta Unije.

2. Komisija objavljuje popis tijela prijavljenih na temelju ove Uredbe, uključujući njihove identifikacijske brojeve i aktivnosti za koje su prijavljena. Komisija osigurava ažuriranje tog popisa.

Članak 36.

Promjene u vezi s prijavama

1. Tijelo koje provodi prijavljivanje obavješćuje Komisiju i druge države članice o svim relevantnim promjenama u vezi s prijavom prijavljenog tijela pomoću alata za elektroničko prijavljivanje iz članka 30. stavka 2.

2. Postupci utvrđeni u člancima 29. i 30. primjenjuju se na proširenja opsega prijave.

Na promjene u vezi s prijavom, uz iznimku proširenja njezina opsega, primjenjuju se postupci utvrđeni u stavcima od 3. do 9.

3. Ako prijavljeno tijelo odluči prestati obavljati aktivnosti ocjenjivanja sukladnosti, o tome obavješćuje tijelo koje provodi prijavljivanje i dotične dobavljače u najkraćem mogućem roku, a u slučaju planiranog prestanka obavljanja aktivnosti barem godinu dana prije prestanka obavljanja svojih aktivnosti. Potvrde prijavljenog tijela mogu ostati valjane tijekom razdoblja od devet mjeseci nakon prestanka obavljanja aktivnosti prijavljenog tijela pod uvjetom da je neko drugo prijavljeno tijelo u pisanom obliku potvrdilo da će preuzeti odgovornost za visokorizične UI sustave na koje se te potvrde odnose. Potonje prijavljeno tijelo provodi cjelovito ocjenjivanje dotičnih visokorizičnih UI sustava do kraja tog devetomjesečnog razdoblja prije nego što izda nove potvrde za te sustave. Ako je prijavljeno tijelo prestalo obavljati svoje aktivnosti, tijelo koje provodi prijavljivanje povlači imenovanje.

4. Ako tijelo koje provodi prijavljivanje ima dovoljno razloga smatrati da određeno prijavljeno tijelo više ne ispunjava zahtjeve utvrđene u članku 31. ili da ne ispunjava svoje obveze, tijelo koje provodi prijavljivanje bez odgode i uz najveću moguću pozornost istražuje to pitanje. U tom kontekstu tijelo koje provodi prijavljivanje obavješćuje dotično prijavljeno tijelo o podnesenim prigovorima i daje mu mogućnost da se izjasni. Ako tijelo koje provodi prijavljivanje zaključi da prijavljeno tijelo više ne ispunjava zahtjeve utvrđene u članku 31. ili da ne ispunjava svoje obveze, ono prema potrebi ograničava, suspendira ili povlači imenovanje, ovisno o težini neispunjavanja tih zahtjeva ili obveza. Tijelo koje provodi prijavljivanje o tome odmah obavješćuje Komisiju i druge države članice.
5. Ako je imenovanje prijavljenog tijela suspendirano, ograničeno ili djelomično ili potpuno povučeno, to tijelo o tome obavješćuje dotične dobavljače u roku od deset dana.
6. U slučaju ograničenja, suspenzije ili povlačenja imenovanja, tijelo koje provodi prijavljivanje poduzima odgovarajuće mjere kako bi osiguralo da se spisi dotičnog prijavljenog tijela sačuvaju te da se stave na raspolaganje tijelima koja provode prijavljivanje u drugim državama članicama i tijelima za nadzor tržišta na njihov zahtjev.
7. U slučaju ograničenja, suspenzije ili povlačenja imenovanja, tijelo koje provodi prijavljivanje:
- (a) ocjenjuje učinak koji to ima na potvrde koje je izdalo prijavljeno tijelo;
 - (b) Komisiji i drugim državama članicama podnosi izvješće o svojim nalazima u roku od tri mjeseca nakon što ih je obavijestilo o promjenama u vezi s imenovanjem;

- (c) od prijavljenog tijela zahtijeva da u razumnom roku koji odredi tijelo koje provodi prijavljivanje suspendira ili povuče sve nepropisno izdane potvrde kako bi se osigurala kontinuirana sukladnost visokorizičnih UI sustava na tržištu;
- (d) obavješćuje Komisiju i države članice o potvdama za koje je zatražilo suspenziju ili povlačenje;
- (e) nacionalnim nadležnim tijelima države članice u kojoj dobavljač ima registrirano mjesto poslovanja dostavlja sve relevantne informacije o potvdama za koje je zatražilo suspenziju ili povlačenje; to tijelo prema potrebi poduzima odgovarajuće mjere kako bi se izbjegao potencijalni rizik za zdravlje, sigurnost ili temeljna prava.

8. Osim ako su potvrde nepropisno izdane i ako je imenovanje suspendirano ili ograničeno, potvrde ostaju valjane u jednoj od sljedećih okolnosti:

- (a) tijelo koje provodi prijavljivanje potvrdilo je, u roku od mjesec dana od suspenzije ili ograničenja, da potvrde na koje se odnosi suspenzija ili ograničenje ne predstavljaju rizik za zdravlje, sigurnost ili temeljna prava te je navelo vremenski raspored za mjere s pomoću kojih bi se suspenzija ili ograničenje mogli ispraviti; ili

- (b) tijelo koje provodi prijavljivanje potvrdilo je da se tijekom razdoblja suspenzije ili ograničenja neće izdavati, mijenjati ili ponovno izdavati potvrde na koje se odnosi suspenzija te navodi je li prijavljeno tijelo sposobno nastaviti pratiti već izdane potvrde i odgovarati za njih tijekom razdoblja suspenzije ili ograničenja. U slučaju da tijelo koje provodi prijavljivanje utvrdi da prijavljeno tijelo nije sposobno dati podršku za već izdane potvrde, dobavljač sustava na koji se potvrda odnosi u roku od tri mjeseca od suspenzije ili ograničenja u pisanom obliku potvrđuje nacionalnim nadležnim tijelima države članice u kojoj ima registrirano mjesto poslovanja da neko drugo kvalificirano prijavljeno tijelo privremeno preuzima funkcije prijavljenog tijela u pogledu praćenja potvrda i odgovaranja za njih tijekom razdoblja suspenzije ili ograničenja.

9. Osim ako su potvrde nepropisno izdane i ako je imenovanje povučeno, potvrde ostaju valjane tijekom razdoblja od devet mjeseci u sljedećim okolnostima:

- (a) nacionalno nadležno tijelo države članice u kojoj dobavljač visokorizičnog UI sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja potvrdilo je da dotični visokorizični UI sustavi ne predstavljaju rizik za zdravlje, sigurnost ili temeljna prava; i
- (b) drugo prijavljeno tijelo potvrdilo je u pisanom obliku da će preuzeti izravnu odgovornost za te UI sustave i da će dovršiti njihovo ocjenjivanje u roku od dvanaest mjeseci od povlačenja imenovanja.

U okolnostima iz prvog podstavka nacionalno nadležno tijelo države članice u kojoj dobavljač sustava na koji se potvrda odnosi ima registrirano mjesto poslovanja može produljiti privremenu valjanost potvrda za dodatna razdoblja od tri mjeseca, pri čemu ukupno razdoblje ne smije biti dulje od 12 mjeseci.

Nacionalno nadležno tijelo ili prijavljeno tijelo koje preuzima funkcije prijavljenog tijela na koje se odnosi promjena u vezi s imenovanjem odmah o tome obavješćuje Komisiju, druge države članice i druga prijavljena tijela.

Članak 37.

Osporavanje stručnosti prijavljenih tijela

1. Komisija prema potrebi istražuje sve slučajeve u kojima postoje razlozi za sumnju u stručnost prijavljenog tijela ili u to da prijavljeno tijelo kontinuirano ispunjava zahtjeve utvrđene u članku 31. i svoje konkretne odgovornosti.
2. Tijelo koje provodi prijavljivanje Komisiji na zahtjev dostavlja sve relevantne informacije koje se odnose na prijavu ili održavanje stručnosti dotičnog prijavljenog tijela.
3. Komisija osigurava da se sa svim osjetljivim informacijama pribavljenima tijekom njezinih istraga na temelju ovog članka postupa na povjerljiv način u skladu s člankom 78.

4. Ako Komisija utvrdi da prijavljeno tijelo ne ispunjava ili da više ne ispunjava zahtjeve za svoju prijavu, o tome obavješćuje državu članicu koja provodi prijavljivanje i od nje zahtijeva da poduzme potrebne korektivne mjere, uključujući suspenziju ili povlačenje prijave ako je to potrebno. Ako država članica ne provede potrebne korektivne mjere, Komisija može provedbenim aktom suspendirati, ograničiti ili povući imenovanje. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

Članak 38.

Koordinacija prijavljenih tijela

1. Komisija osigurava da se u vezi s visokorizičnim UI sustavima uspostave i pravilno provode primjerena koordinacija i suradnja prijavljenih tijela koja se bave postupcima ocjenjivanja sukladnosti na temelju ove Uredbe, i to u okviru sektorske skupine prijavljenih tijela.
2. Svako tijelo koje provodi prijavljivanje osigurava da tijela koja je prijavilo sudjeluju u radu skupine iz stavka 1., izravno ili preko imenovanih predstavnika.
3. Komisija osigurava razmjenu znanja i primjera najbolje prakse među tijelima koja provode prijavljivanje.

Članak 39.

Tijela za ocjenjivanje sukladnosti iz trećih zemalja

Tijela za ocjenjivanje sukladnosti uspostavljena na temelju prava određene treće zemlje s kojom je Unija sklopila sporazum mogu biti ovlaštena za obavljanje aktivnosti prijavljenih tijela na temelju ove Uredbe, pod uvjetom da ispunjavaju zahtjeve utvrđene u članku 31. ili osiguraju jednakovrijednu razinu usklađenosti.

ODJELJAK 5.

NORME, OCJENJIVANJE SUKLADNOSTI, POTVRDE, REGISTRACIJA

Članak 40.

Usklađene norme i normizacijski dokumenti

1. Za visokorizične UI sustave ili UI modele opće namjene koji su sukladni s usklađenim normama ili dijelovima usklađenih normi na koje su objavljena upućivanja u *Službenom listu Europske unije* u skladu s Uredbom (EU) br. 1025/2012 pretpostavlja se da su sukladni sa zahtjevima utvrđenima u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, s obvezama utvrđenima u poglavlju V. odjeljcima 2. i 3. ove Uredbe, u mjeri u kojoj te norme obuhvaćaju te zahtjeve ili obveze.

2. U skladu s člankom 10. Uredbe (EU) br. 1025/2012 Komisija bez nepotrebne odgode upućuje zahtjeve za normizaciju koji obuhvaćaju sve zahtjeve utvrđene u odjeljku 2. ovog poglavlja i, ovisno o slučaju, zahtjeve za normizaciju koji obuhvaćaju obveze utvrđene u poglavlju V. odjeljcima 2. i 3. ove Uredbe. U okviru zahtjeva za normizaciju također se zahtijeva izrada dokumenata u vezi s procesom izvješćivanja i dokumentiranja kako bi se poboljšala resursna učinkovitost UI sustavâ, primjerice kako bi visokorizični UI sustav smanjio potrošnju energije i drugih resursa tijekom svojeg životnog ciklusa, te u vezi s energetske učinkovitim razvojem UI modelâ opće namjene. Pri izradi zahtjeva za normizaciju Komisija se savjetuje s Vijećem za umjetnu inteligenciju i relevantnim dionicima, uključujući savjetodavni forum.

Pri upućivanju zahtjeva za normizaciju europskim organizacijama za normizaciju Komisija navodi da norme moraju biti jasne i usklađene, među ostalim i s normama razvijenima u raznim sektorima za proizvode obuhvaćene postojećim zakonodavstvom Unije o usklađivanju navedenim u Prilogu I., i da se njima mora osigurati da visokorizični UI sustavi ili UI modeli opće namjene koji se stavljaju na tržište ili u upotrebu u Uniji ispunjavaju relevantne zahtjeve ili obveze utvrđene u ovoj Uredbi.

Komisija također zahtijeva od europskih organizacija za normizaciju da dostave dokaze o svojim nastojanjima da ispune ciljeve iz prvog i drugog podstavka ovog stavka u skladu s člankom 24. Uredbe (EU) br. 1025/2012.

3. Sudionici u procesu normizacije nastoje promicati ulaganja i inovacije u području umjetne inteligencije, među ostalim povećanjem pravne sigurnosti, kao i konkurentnosti i rasta tržišta Unije, te doprinositi jačanju globalne suradnje u području normizacije, uzimajući u obzir postojeće međunarodne norme u području umjetne inteligencije koje su u skladu s vrijednostima, temeljnim pravima i interesima Unije, i poboljšati višedioničko upravljanje osiguravanjem ujednačene zastupljenosti interesa i djelotvornog sudjelovanja svih relevantnih dionika u skladu s člancima 5., 6. i 7. Uredbe (EU) br. 1025/2012.

Članak 41.

Zajedničke specifikacije

1. Komisija može donositi provedbene akte o utvrđivanju zajedničkih specifikacija za zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, za obveze utvrđene u odjeljcima 2. i 3. poglavlja V. ako su ispunjeni sljedeći uvjeti:
 - (a) Komisija je na temelju članka 10. stavka 1. Uredbe (EU) br. 1025/2012 zatražila od jedne ili više europskih organizacija za normizaciju da izrade usklađenu normu za zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, za obveze utvrđene u odjeljcima 2. i 3. poglavlja V., a:
 - i. zahtjev nije prihvatila nijedna europska organizacija za normizaciju; ili

- ii. usklađene norme koje se odnose na taj zahtjev nisu izrađene u roku utvrđenom u skladu s člankom 10. stavkom 1. Uredbe (EU) br. 1025/2012; ili
 - iii. relevantnim usklađenim normama nisu dostatno uvažena pitanja temeljnih prava; ili
 - iv. usklađene norme nisu u skladu sa zahtjevom; i
- (b) u *Službenom listu Europske unije* nije objavljeno, u skladu s Uredbom (EU) br. 1025/2012, upućivanje na usklađene norme koje obuhvaćaju zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, obveze utvrđene u odjeljcima 2. i 3. poglavlja V., niti se očekuje objava takvih upućivanja u razumnom roku.

Pri izradi zajedničkih specifikacija Komisija se savjetuje sa savjetodavnim forumom iz članka 67.

Provedbeni akti iz prvog podstavka ovog stavka donose se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

2. Prije nego što izradi nacrt provedbenog akta Komisija obavještuje odbor iz članka 22. Uredbe (EU) br. 1025/2012 o tome da smatra da su uvjeti utvrđeni u stavku 1. ovog članka ispunjeni.

3. Za visokorizične UI sustave ili UI modele opće namjene koji su sukladni sa zajedničkim specifikacijama iz stavka 1. ili dijelovima tih specifikacija pretpostavlja se da su sukladni sa zahtjevima utvrđenima u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, da su u skladu s obvezama utvrđenima u odjeljcima 2. i 3. poglavlja V., u mjeri u kojoj te zajedničke specifikacije obuhvaćaju te zahtjeve ili te obveze.
4. Ako europska organizacija za normizaciju donese usklađenu normu i Komisiji predloži da se upućivanje na nju objavi u *Službenom listu Europske unije*, Komisija ocjenjuje tu usklađenu normu u skladu s Uredbom (EU) br. 1025/2012. Kad se upućivanje na usklađenu normu objavi u *Službenom listu Europske unije*, Komisija stavlja izvan snage provedbene akte iz stavka 1. ili njihove dijelove koji obuhvaćaju iste zahtjeve utvrđene u odjeljku 2. ovog poglavlja odnosno, ovisno o slučaju, iste obveze utvrđene u odjeljcima 2. i 3. poglavlja V.
5. Ako dobavljači visokorizičnih UI sustava ili UI modela opće namjene ne ispunjavaju zajedničke specifikacije iz stavka 1., moraju propisno obrazložiti da su usvojili tehnička rješenja kojima se ispunjavaju zahtjevi iz odjeljka 2. ovog poglavlja odnosno, ovisno o slučaju, kojima se ispunjavaju obveze utvrđene u odjeljcima 2. i 3. poglavlja V., na razini koja je barem jednakovrijedna tim zajedničkim specifikacijama.

6. Ako država članica smatra da zajednička specifikacija ne ispunjava u potpunosti zahtjeve utvrđene u odjeljku 2. odnosno, ovisno o slučaju, obveze utvrđene u odjeljcima 2. i 3. poglavlja V., ona o tome obavještuje Komisiju i navodi detaljno objašnjenje. Komisija ocjenjuje te informacije i, prema potrebi, mijenja provedbeni akt kojim se utvrđuje dotična zajednička specifikacija.

Članak 42.

Pretpostavka sukladnosti s određenim zahtjevima

1. Za visokorizične UI sustave koji su trenirani i testirani na podacima koji odražavaju specifično zemljopisno, bihevioralno, kontekstualno ili radno okružje u kojem se namjeravaju koristiti pretpostavlja se da ispunjavaju relevantne zahtjeve utvrđene u članku 10. stavku 4.
2. Za visokorizične UI sustave koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibernetičke sigurnosti na temelju Uredbe (EU) 2019/881 i na koje su objavljena upućivanja u *Službenom listu Europske unije* pretpostavlja se da ispunjavaju zahtjeve u pogledu kibernetičke sigurnosti iz članka 15. ove Uredbe ako certifikat o kibernetičkoj sigurnosti ili izjava o sukladnosti ili njihovi dijelovi obuhvaćaju te zahtjeve.

Članak 43.

Ocjenjivanje sukladnosti

1. U vezi s visokorizičnim UI sustavima iz točke 1. Priloga III., ako je dobavljač pri dokazivanju usklađenosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. primijenio usklađene norme iz članka 40. ili, ako je primjenjivo, zajedničke specifikacije iz članka 41., dobavljač bira jedan od sljedećih postupaka ocjenjivanja sukladnosti na temelju:

- (a) unutarnje kontrole iz Priloga VI.; ili
- (b) ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije iz Priloga VII., uz sudjelovanje prijavljenog tijela.

Pri dokazivanju usklađenosti visokorizičnog UI sustava sa zahtjevima utvrđenima u odjeljku 2. dobavljač primjenjuje postupak ocjenjivanja sukladnosti iz Priloga VII. ako:

- (a) usklađene norme iz članka 40. ne postoje, a zajedničke specifikacije iz članka 41. nisu dostupne;
- (b) dobavljač nije primijenio usklađenu normu ili je primijenio samo dio usklađene norme;
- (c) zajedničke specifikacije iz točke (a) postoje, ali ih dobavljač nije primijenio;

- (d) jedna ili više usklađenih normi iz točke (a) objavljena je uz ograničenje, i to samo za dio norme koji je ograničen.

Za potrebe postupka ocjenjivanja sukladnosti iz Priloga VII. dobavljač može odabrati bilo koje prijavljeno tijelo. Međutim, ako visokorizični UI sustav u upotrebu namjeravaju staviti tijela kaznenog progona, tijela za imigraciju ili tijela za azil odnosno institucije, tijela, uredi ili agencije Unije, tijelo za nadzor tržišta iz članka 74. stavka 8. ili 9., ovisno o slučaju, djeluje kao prijavljeno tijelo.

2. Za visokorizične UI sustave iz točaka od 2. do 8. Priloga III. dobavljači primjenjuju postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI., kojim se ne predviđa sudjelovanje prijavljenog tijela.
3. Za visokorizične UI sustave obuhvaćene zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I. dobavljač primjenjuje relevantni postupak ocjenjivanja sukladnosti kako se zahtijeva tim pravnim aktima. Na te visokorizične UI sustave primjenjuju se zahtjevi utvrđeni u odjeljku 2. ovog poglavlja i dio su tog ocjenjivanja. Također se primjenjuju točke 4.3., 4.4., 4.5. i točka 4.6. peti odlomak Priloga VII.

Za potrebe tog ocjenjivanja prijavljena tijela koja su prijavljena na temelju tih pravnih akata imaju pravo kontrolirati sukladnost visokorizičnih UI sustava sa zahtjevima utvrđenima u odjeljku 2. pod uvjetom da je u kontekstu postupka prijavljivanja na temelju tih pravnih akata ocijenjeno ispunjavaju li dotična prijavljena tijela zahtjeve utvrđene u članku 31. stavcima 4., 5., 10. i 11.

Ako je pravnim aktom navedenim u odjeljku A Priloga II. proizvođaču proizvoda omogućeno da se izuzme iz ocjenjivanja sukladnosti koje provodi treća strana pod uvjetom da je taj proizvođač primijenio sve usklađene norme koje obuhvaćaju sve relevantne zahtjeve, taj proizvođač tu mogućnost može iskoristiti samo ako je primijenio i usklađene norme ili, ako je primjenjivo, zajedničke specifikacije iz članka 41., koje obuhvaćaju sve zahtjeve utvrđene u odjeljku 2. ovog poglavlja.

4. Za visokorizične UI sustave koji su već bili podvrgnuti postupku ocjenjivanja sukladnosti provodi se novi postupak ocjenjivanja sukladnosti ako dođe do bitnih izmjena, neovisno o tome namjerava li se izmijenjeni sustav dalje distribuirati ili ga nastavlja upotrebljavati isti subjekt koji ga već uvodi.

Za visokorizične UI sustave koji nastavljaju učiti nakon stavljanja na tržište ili u upotrebu, promjene visokorizičnog UI sustava i njegove učinkovitosti koje je dobavljač unaprijed odredio u trenutku početnog ocjenjivanja sukladnosti i koje su obuhvaćene informacijama u tehničkoj dokumentaciji iz točke 2. podtočke (f) Priloga IV. ne čine bitnu izmjenu.

5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene priloga VI. i VII. njihovim ažuriranjem s obzirom na tehnički napredak.

6. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene stavaka 1. i 2. ovog članka kako bi visokorizične UI sustave iz točaka od 2. do 8. Priloga III. podvrgnula postupku ocjenjivanja sukladnosti iz Priloga VII. ili dijelovima tog postupka. Komisija takve delegirane akte donosi uzimajući u obzir djelotvornost postupka ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI. u sprečavanju rizika za zdravlje i sigurnost te zaštitu temeljnih prava koje takvi sustavi predstavljaju ili svođenju takvih rizika na najmanju moguću mjeru, kao i dostupnost adekvatnih kapaciteta i resursa među prijavljenim tijelima.

Članak 44.

Potvrde

1. Potvrde koje izdaju prijavljena tijela u skladu s Prilogom VII. sastavljaju se na jeziku koji relevantna tijela u državi članici u kojoj prijavljeno tijelo ima poslovni nastan mogu bez poteškoća razumjeti.
2. Potvrde vrijede tijekom razdoblja koje je u njima navedeno, a ono ne smije biti dulje od pet godina za UI sustave obuhvaćene Prilogom I. i dulje od četiri godine za UI sustave obuhvaćene Prilogom III. Na zahtjev dobavljača valjanost potvrde može se produljivati za daljnja razdoblja od kojih nijedno ne smije biti dulje od pet godina za UI sustave obuhvaćene Prilogom I. i dulje od četiri godine za UI sustave obuhvaćene Prilogom III., i to na temelju ponovnog ocjenjivanja u skladu s primjenjivim postupcima ocjenjivanja sukladnosti. Svaka dopuna potvrde ostaje valjana pod uvjetom da je valjana potvrda koju dopunjuje.

3. Ako prijavljeno tijelo ustanovi da UI sustav više ne ispunjava zahtjeve utvrđene u odjeljku 2., to prijavljeno tijelo, uzimajući u obzir načelo proporcionalnosti, suspendira ili povlači izdanu potvrdu ili uvodi ograničenja za nju, osim ako se primjerenim korektivnim mjerama koje dobavljač sustava poduzme u primjerenom roku koji je utvrdilo prijavljeno tijelo osigura usklađenost UI sustava s tim zahtjevima. Prijavljeno tijelo daje obrazloženje za svoju odluku.

Protiv odluka prijavljenih tijela, među ostalim protiv odluka o izdanim potvrdama o sukladnosti, mora biti dostupan žalbeni postupak.

Članak 45.

Obveze prijavljenih tijela u pogledu obavješćivanja

1. Prijavljena tijela obavješćuju tijelo koje provodi prijavljivanje o sljedećem:
 - (a) potvrdama Unije o ocjenjivanju tehničke dokumentacije, dopunama tih potvrda i odobrenjima sustava upravljanja kvalitetom izdanima u skladu sa zahtjevima iz Priloga VII.;
 - (b) odbijanju, ograničenju, suspenziji ili povlačenju potvrde Unije o ocjenjivanju tehničke dokumentacije ili odobrenja sustava upravljanja kvalitetom izdanog u skladu sa zahtjevima iz Priloga VII.;
 - (c) svim okolnostima koje utječu na opseg prijavljivanja ili uvjete za prijavljivanje;

- (d) zahtjevima za dostavu informacija koje su primila od tijela za nadzor tržišta u vezi s aktivnostima ocjenjivanja sukladnosti;
 - (e) na zahtjev, o aktivnostima ocjenjivanja sukladnosti provedenima u okviru njihove prijave i svim ostalim provedenim aktivnostima, uključujući prekogranične aktivnosti i podugovaranje.
2. Svako prijavljeno tijelo obavještuje druga prijavljena tijela o sljedećem:
- (a) odobrenjima sustava upravljanja kvalitetom koja je odbilo, suspendiralo ili povuklo i, na zahtjev, odobrenjima sustava upravljanja kvalitetom koja je izdalo;
 - (b) potvrdama Unije o ocjenjivanju tehničke dokumentacije ili dopunama tih potvrda koje je odbilo, povuklo, suspendiralo ili na neki drugi način ograničilo te, na zahtjev, potvrdama i/ili njihovim dopunama koje je izdalo.
3. Svako prijavljeno tijelo drugim prijavljenim tijelima koja provode slične aktivnosti ocjenjivanja sukladnosti za iste vrste UI sustava dostavlja relevantne informacije o pitanjima povezanim s negativnim i, na zahtjev, pozitivnim rezultatima ocjenjivanja sukladnosti.
4. Prijavljena tijela u skladu s člankom 78. štite povjerljivost informacija koje su pribavila.

Članak 46.

Odstupanje od postupka ocjenjivanja sukladnosti

1. Odstupajući od članka 43., i na propisno obrazložen zahtjev, svako tijelo za nadzor tržišta može odobriti stavljanje određenih visokorizičnih UI sustava na tržište ili u upotrebu na državnom području dotične države članice zbog iznimnih razloga koji se odnose na javnu sigurnost ili zaštitu života i zdravlja ljudi, zaštitu okoliša ili zaštitu ključne industrijske i infrastrukturne imovine. Trajanje tog odobrenja ograničeno je na razdoblje provedbe potrebnih postupaka ocjenjivanja sukladnosti, uzimajući u obzir iznimne razloge koji opravdavaju odstupanje. Ti se postupci dovršavaju bez nepotrebne odgode.
2. U propisno opravdanoj hitnoj situaciji zbog iznimnih razloga koji se odnose na javnu sigurnost ili u slučaju konkretne, znatne i izravne prijetnje životu ili tjelesnoj sigurnosti fizičkih osoba, tijela kaznenog progona ili tijela civilne zaštite mogu određeni visokorizični UI sustav staviti u upotrebu bez odobrenja iz stavka 1. pod uvjetom da se to odobrenje bez nepotrebne odgode zatraži tijekom ili nakon upotrebe. Ako je odobrenje iz stavka 1. odbijeno, upotreba visokorizičnog UI sustava smjesta se prekida te se odmah odbacuju svi rezultati i izlazni podaci proizašli iz takve upotrebe.

3. Odobrenje iz stavka 1. izdaje se samo ako tijelo za nadzor tržišta zaključi da visokorizični UI sustav ispunjava zahtjeve iz odjeljka 2. Tijelo za nadzor tržišta obavještuje Komisiju i druge države članice o svim odobrenjima izdanim na temelju stavaka 1 i 2. Ta obveza ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona.
4. Ako u roku od 15 kalendarskih dana od primitka informacija iz stavka 3. nijedna država članica ni Komisija ne podnese prigovor na odobrenje koje je izdalo tijelo za nadzor tržišta određene države članice u skladu sa stavkom 1., to se odobrenje smatra opravdanim.
5. Ako u roku od 15 kalendarskih dana od primitka obavijesti iz stavka 3. određena država članica podnese prigovor na odobrenje koje je izdalo tijelo za nadzor tržišta druge države članice ili ako Komisija smatra da je to odobrenje u suprotnosti s pravom Unije ili da je zaključak država članica o usklađenosti sustava iz stavka 3. neosnovan, Komisija bez odgode započinje savjetovanje s relevantnom državom članicom. U savjetovanju sudjeluju dotični operateri i omogućuje im se da iznesu svoja stajališta. Komisija ih uzima u obzir i odlučuje je li odobrenje opravdano. Komisija svoju odluku upućuje dotičnim državama članicama i dotičnim operaterima.
6. Ako Komisija odobrenje smatra neopravdanim, tijelo za nadzor tržišta dotične države članice povlači to odobrenje.

7. Kad je riječ o visokorizičnim UI sustavima koji su povezani s proizvodima obuhvaćenima zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., primjenjuju se samo odstupanja od ocjenjivanja sukladnosti utvrđena u tom zakonodavstvu Unije o usklađivanju.

Članak 47.

EU izjava o sukladnosti

1. Dobavljač sastavlja pisanu, strojno čitljivu EU izjavu o sukladnosti, potpisanu fizički ili elektronički, za svaki visokorizični UI sustav i drži je na raspolaganju nacionalnim nadležnim tijelima tijekom razdoblja od deset godina nakon stavljanja tog visokorizičnog UI sustava na tržište ili u upotrebu. U EU izjavi o sukladnosti navodi se za koji je visokorizični UI sustav ona sastavljena. Primjerak EU izjave o sukladnosti dostavlja se relevantnim nacionalnim nadležnim tijelima na njihov zahtjev.
2. U EU izjavi o sukladnosti navodi se da dotični visokorizični UI sustav ispunjava zahtjeve utvrđene u odjeljku 2. EU izjava o sukladnosti sadržava informacije utvrđene u Prilogu V. i prevodi se na jezik koji nacionalna nadležna tijela država članica u kojima se visokorizični UI sustav stavlja na tržište ili na raspolaganje mogu bez poteškoća razumjeti.

3. Ako visokorizični UI sustavi podliježu drugom zakonodavstvu Unije o usklađivanju kojim se također zahtijeva EU izjava o sukladnosti, sastavlja se jedinstvena EU izjava o sukladnosti koja se odnosi na svo pravo Unije koje se primjenjuje na dotični visokorizični UI sustav. Ta izjava sadržava sve informacije potrebne za identifikaciju zakonodavstva Unije o usklađivanju na koje se izjava odnosi.
4. Sastavljanjem EU izjave o sukladnosti dobavljač preuzima odgovornost za ispunjavanje zahtjeva utvrđenih u odjeljku 2. Dobavljač prema potrebi ažurira EU izjavu o sukladnosti.
5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene Priloga V. ažuriranjem sadržaja EU izjave o sukladnosti utvrđene u tom prilogu kako bi se uveli elementi koji postanu potrebni s obzirom na tehnički napredak.

Članak 48.

Oznaka CE

1. Za oznaku CE vrijede opća načela utvrđena u članku 30. Uredbe (EZ) br. 765/2008.
2. Za visokorizične UI sustave koji se pružaju digitalno digitalna oznaka CE upotrebljava se samo ako joj se može lako pristupiti preko sučelja s kojeg se pristupa tom sustavu ili s pomoću lako dostupnog strojno čitljivog koda ili drugih elektroničkih sredstava.

3. Oznaka CE stavlja se na visokorizične UI sustave tako da bude vidljiva, čitka i neizbrisiva. Ako to zbog prirode visokorizičnog UI sustava nije moguće ili nije opravdano, oznaka CE stavlja se na pakiranje ili na popratnu dokumentaciju, ovisno o slučaju.
4. Ako je primjenjivo, uz oznaku CE navodi se identifikacijski broj prijavljenog tijela odgovornog za postupke ocjenjivanja sukladnosti iz članka 43. Identifikacijski broj prijavljenog tijela stavlja sâmo prijavljeno tijelo ili ga prema njegovim uputama stavlja dobavljač ili dobavljačev ovlašteni zastupnik. Taj identifikacijski broj navodi se i u svim promotivnim materijalima u kojima se navodi da dotični visokorizični UI sustav ispunjava zahtjeve u pogledu oznake CE.
5. Ako visokorizični UI sustavi podliježu drugom pravu Unije kojim se također predviđa stavljanje oznake CE, na oznaci CE navodi se da visokorizični UI sustav ispunjava i zahtjeve iz tog drugog prava.

Članak 49.

Registracija

1. Prije stavljanja na tržište ili u upotrebu visokorizičnog UI sustava iz Priloga III., uz izuzeće visokorizičnih UI sustava iz točke 2. Priloga III., dobavljač ili, ako je primjenjivo, ovlašteni zastupnik registrira sebe i svoj sustav u bazi podataka EU-a iz članka 71.

2. Prije stavljanja na tržište ili u upotrebu UI sustava za koji je dobavljač zaključio da nije visokorizičan u skladu s člankom 6. stavkom 3., taj dobavljač ili, ako je primjenjivo, ovlašteni zastupnik registrira sebe i taj sustav u bazi podataka EU-a iz članka 71.
3. Prije stavljanja u upotrebu ili korištenja visokorizičnog UI sustava iz Priloga III., uz izuzeće visokorizičnih UI sustava iz točke 2. Priloga III., subjekti koji uvode sustav koji su tijela javne vlasti, institucije, tijela uredi ili agencije Unije ili osobe koje djeluju u njihovo ime registriraju se, odabiru sustav i registriraju njegovo korištenje u bazi podataka EU-a iz članka 71.
4. Za visokorizične UI sustave iz točaka 1., 6. i 7. Priloga III., u području kaznenog progona, migracija, azila i upravljanja nadzorom državne granice registracija iz stavaka 1., 2. i 3. ovog članka provodi se u sigurnom dijelu baze podataka EU-a iz članka 71. koji nije javno dostupan, a uključuje samo informacije iz sljedećega, ovisno o slučaju:
 - (a) odjeljka A točaka od 1. do 10. Priloga VIII., osim točaka 6., 8. i 9.;
 - (b) odjeljka B točaka od 1. do 5. i točaka 8. i 9. Priloga VIII.;
 - (c) odjeljka C točaka od 1. do 3. Priloga VIII.;
 - (d) točaka 1., 2., 3. i 5. Priloga IX.

Samo Komisija i nacionalna tijela iz članka 74. stavka 8. imaju pristup odgovarajućim dijelovima baze podataka EU-a kojima je pristup ograničen, a koji su navedeni u prvom podstavku ovog stavka.

5. Visokorizični UI sustavi iz točke 2. Priloga III. registriraju se na nacionalnoj razini.

Poglavlje IV.

Obveze u pogledu transparentnosti za dobavljače određenih UI sustava i subjekte koji ih uvode

Članak 50.

Obveze u pogledu transparentnosti za dobavljače određenih UI sustava i subjekte koji ih uvode

1. Dobavljači osiguravaju da su UI sustavi koji su namijenjeni izravnoj interakciji s fizičkim osobama dizajnirani i razvijeni na takav način da se dotične fizičke osobe obavješćuje o tome da su u interakciji s UI sustavom, osim ako je to očito sa stajališta razmjerno dobro informirane, pronicljive i oprezne fizičke osobe, uzimajući u obzir okolnosti i kontekst upotrebe. Ta se obveza ne primjenjuje na UI sustave koji su zakonski odobreni za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana, osim ako su ti sustavi dostupni javnosti za prijavu kaznenih djela.

2. Dobavljači UI sustava, uključujući UI sustave opće namjene, koji generiraju sintetički audiosadržaj, slikovni sadržaj, videosadržaj ili tekstovni sadržaj osiguravaju da izlazni rezultati UI sustava budu označeni u strojno čitljivom obliku i da ih se može prepoznati kao umjetno generirane ili manipulirane. Dobavljači osiguravaju da njihova tehnička rješenja budu djelotvorna, interoperabilna, otporna i pouzdana u mjeri u kojoj je to tehnički izvedivo, uzimajući u obzir posebnosti i ograničenja različitih vrsta sadržaja, troškove provedbe i općepriznata najnovija dostignuća, što se može odražavati u relevantnim tehničkim normama. Ta se obveza ne primjenjuje ako UI sustavi obavljaju pomoćnu funkciju za standardno uređivanje ili bitno ne mijenjaju ulazne podatke koje pruža subjekt koji uvodi sustav ili njihovu semantiku, ili ako su zakonski odobreni za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela.
3. Subjekti koji uvode sustav za prepoznavanje emocija ili sustav za biometrijsku kategorizaciju obavješćuju fizičke osobe koje su izložene tom sustavu o njegovu radu, a osobne podatke obrađuju u skladu s uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivom (EU) 2016/680, ovisno o slučaju. Ta se obveza ne primjenjuje na UI sustave za biometrijsku kategorizaciju i prepoznavanje emocija koji su zakonski odobreni za otkrivanje, sprečavanje ili istragu kaznenih djela, podložno odgovarajućim zaštitnim mjerama za prava i slobode trećih strana i u skladu s pravom Unije.

4. Subjekti koji uvode UI sustav koji generira ili manipulira slikovnim sadržajem, audiosadržajem ili videosadržajem koji čini uvjerljiv krivotvoreni sadržaj (*deep fake*) moraju navesti da je taj sadržaj umjetno generiran ili da je njime manipulirano. Ta se obveza ne primjenjuje ako je korištenje zakonski odobreno za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela. Ako je sadržaj dio očigledno umjetničkog, kreativnog, satiričnog, fiktivnog ili analognog djela ili programa, obveze u pogledu transparentnosti iz ovog stavka ograničene su na otkrivanje postojanja takvog generiranog ili manipuliranog sadržaja na odgovarajući način kojim se ne ometa prikazivanje tog djela ili uživanje u njemu.

Subjekti koji uvode UI sustav koji generira ili manipulira tekстом koji se objavljuje u svrhu informiranja javnosti o pitanjima od javnog interesa moraju navesti da je tekst umjetno generiran ili da je njime manipulirano. Ta se obveza ne primjenjuje ako je korištenje zakonski odobreno za otkrivanje, sprečavanje, istragu ili kazneni progon kaznenih djela ili ako je sadržaj generiran umjetnom inteligencijom prošao proces preispitivanja koje provodi čovjek ili uredničku kontrolu i ako fizička ili pravna osoba snosi uredničku odgovornost za objavu sadržaja.

5. Informacije iz stavaka od 1. do 4. dotičnim se fizičkim osobama pružaju na jasan i raspoznatljiv način najkasnije u trenutku prve interakcije ili prvog izlaganja. Te informacije moraju ispunjavati primjenjive zahtjeve u pogledu pristupačnosti.
6. Stavci od 1. do 4. ne utječu na zahtjeve i obveze iz poglavlja III. i njima se ne dovode u pitanje druge obveze u pogledu transparentnosti utvrđene u pravu Unije ili nacionalnom pravu za subjekte koji uvode UI sustave.

7. Ured za umjetnu inteligenciju potiče i olakšava izradu kodeksâ prakse na razini Unije kako bi se olakšala djelotvorna provedba obveza u pogledu otkrivanja i označivanja umjetno generiranog ili manipuliranog sadržaja. Komisija može donositi provedbene akte radi odobravanja tih kodeksa prakse u skladu s postupkom utvrđenim u članku 56. stavku 6. Ako smatra da kodeks nije adekvatan, Komisija može donositi provedbene akte o utvrđivanju zajedničkih pravila za provedbu tih obveza u skladu s postupkom ispitivanja utvrđenim u članku 98. stavku 2.

Poglavlje V.

UI modeli opće namjene

ODJELJAK 1.

PRAVILA O KLASIFIKACIJI

Članak 51.

Klasifikacija UI modela opće namjene kao UI modela opće namjene sa sistemskim rizikom

1. UI model opće namjene klasificira se kao UI model opće namjene sa sistemskim rizikom ako ispunjava bilo koji od sljedećih uvjeta:
 - (a) ima sposobnosti visokog učinka evaluirane na temelju odgovarajućih tehničkih alata i metodologija, uključujući pokazatelje i referentne vrijednosti;

- (b) na temelju odluke Komisije, po službenoj dužnosti ili slijedom kvalificiranog upozorenja znanstvenog povjerenstva, ima sposobnosti ili učinak jednakovrijedne onima utvrđenima u točki (a), uzimajući u obzir kriterije utvrđene u Prilogu XIII.
2. Pretpostavlja se da UI model opće namjene ima sposobnosti visokog učinka u skladu sa stavkom 1. točkom (a) ako je kumulativna količina računanja korištena za njegovo treniranje iskazana brojem matematičkih operacija nad brojevima s pomičnim zarezom u sekundi veća od 10^{25} .
3. Komisija donosi delegirane akte u skladu s člankom 97. radi izmjene pragova navedenih u stavcima 1. i 2. ovog članka te, prema potrebi, radi dopune referentnih vrijednosti i pokazatelja s obzirom na tehnološki razvoj, kao što su algoritamska poboljšanja ili povećanje učinkovitosti hardvera, kako bi ti pragovi odražavali najnovija dostignuća.

Članak 52.

Postupak

1. Ako UI model opće namjene ispunjava uvjet iz članka 51. stavka 1. točke (a), dotični dobavljač o tome obavješćuje Komisiju bez odgode, a u svakom slučaju u roku od dva tjedna nakon što je taj zahtjev ispunjen ili nakon što postane poznato da će biti ispunjen. Ta obavijest uključuje informacije potrebne kako bi se dokazalo da je dotični zahtjev ispunjen. Ako Komisija sazna za UI model opće namjene koji predstavlja sistemske rizike, a o kojem nije bila obaviještena, može ga odlučiti odrediti kao model sa sistemskim rizikom.

2. Dobavljač UI modela opće namjene koji ispunjava uvjet iz članka 51. stavka 1. točke (a) može uz svoju obavijest dostaviti dostatno potkrijepljene argumente kako bi dokazao da UI model opće namjene iznimno, iako ispunjava navedeni zahtjev, zbog svojih specifičnih karakteristika ne predstavlja sistemske rizike i da ga stoga ne bi trebalo klasificirati kao UI model opće namjene sa sistemskim rizikom.
3. Ako Komisija zaključi da argumenti dostavljeni na temelju stavka 2. nisu dostatno potkrijepljeni i da dotični dobavljač nije dokazao da UI model opće namjene zbog svojih specifičnih karakteristika ne predstavlja sistemske rizike, ona odbacuje te argumente, a UI model opće namjene smatra se UI modelom opće namjene sa sistemskim rizikom.
4. Komisija može UI model opće namjene odrediti kao model koji predstavlja sistemske rizike na temelju kriterija iz Priloga XIII., po službenoj dužnosti ili slijedom kvalificiranog upozorenja znanstvenog povjerenstva u skladu s člankom 90. stavkom 1. točkom (a).

Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. radi izmjene Priloga XIII. utvrđivanjem i ažuriranjem kriterija utvrđenih u tom prilogu.

5. Na obrazloženi zahtjev dobavljača čiji je model u skladu sa stavkom 4. određen kao UI model opće namjene sa sistemskim rizikom, Komisija takav zahtjev uzima u obzir i može odlučiti ponovno ocijeniti može li se i dalje smatrati da UI model opće namjene predstavlja sistemske rizike na temelju kriterija iz Priloga XIII. Takav zahtjev mora sadržavati objektivne, detaljne i nove razloge koji su se pojavili nakon odluke o određivanju. Dobavljači mogu zatražiti ponovnu ocjenu najranije šest mjeseci nakon odluke o određivanju. Ako Komisija nakon ponovne ocjene odluči zadržati određivanje modela kao UI modela opće namjene sa sistemskim rizikom, dobavljači mogu zatražiti ponovno ocjenjivanje najranije šest mjeseci nakon te odluke.
6. Komisija osigurava objavljivanje popisa UI modelâ opće namjene sa sistemskim rizikom i ažurira ga, ne dovodeći u pitanje potrebu za poštovanjem i zaštitom prava intelektualnog vlasništva i povjerljivih poslovnih informacija ili poslovnih tajni u skladu s pravom Unije i nacionalnim pravom.

ODJELJAK 2.

OBVEZE DOBAVLJAČA UI MODELÂ OPĆE NAMJENE

Članak 53.

Obveze dobavljača UI modelâ opće namjene

1. Dobavljači UI modelâ opće namjene:
 - (a) izrađuju i ažuriraju tehničku dokumentaciju modela, među ostalim o postupku njegova treniranja i testiranja te rezultatima njegove evaluacije, koja sadržava barem informacije utvrđene u Prilogu XI., kako bi je na zahtjev dostavili Uredu za umjetnu inteligenciju i nacionalnim nadležnim tijelima;
 - (b) izrađuju, ažuriraju i stavljaju na raspolaganje informacije i dokumentaciju dobavljačima UI sustava koji namjeravaju integrirati UI model opće namjene u svoje UI sustave. Ne dovodeći u pitanje potrebu za poštovanjem i zaštitom prava intelektualnog vlasništva i povjerljivih poslovnih informacija ili poslovnih tajni u skladu s pravom Unije i nacionalnim pravom, te informacije i dokumentacija:
 - i. omogućuju dobavljačima UI sustava da dobro razumiju sposobnosti i ograničenja UI modela opće namjene i da ispune svoje obveze na temelju ove Uredbe; i
 - ii. sadržavaju barem elemente utvrđene u Prilogu XII.;

- (c) uspostavljaju politiku usklađivanja s pravom Unije o autorskom pravu i povezanim pravima, posebno kako bi utvrdili i poštovali, među ostalim i s pomoću najsuvremenijih tehnologija, pridržaj prava izražen u skladu s člankom 4. stavkom 3. Direktive (EU) 2019/790;
 - (d) izrađuju i objavljuju dovoljno detaljan sažetak o sadržaju upotrijebljenom za treniranje UI modela opće namjene, prema predlošku Ureda za umjetnu inteligenciju.
2. Obveze utvrđene u stavku 1. točkama (a) i (b) ne primjenjuju se na dobavljače UI modela koji se objavljuju na temelju besplatne licencije za softver otvorenog koda koja omogućuje pristup modelu te njegovu upotrebu, izmjenu i distribuciju i čiji su parametri, uključujući težinske faktore, informacije o arhitekturi modela te informacije o upotrebi modela, javno dostupni. Ta se iznimka ne primjenjuje na UI modele opće namjene sa sistemskim rizikom.
3. Dobavljači UI modela opće namjene prema potrebi surađuju s Komisijom i nacionalnim nadležnim tijelima u izvršavanju njihovih nadležnosti i ovlasti na temelju ove Uredbe.

4. Dobavljači UI modelâ opće namjene mogu se do objave usklađene norme osloniti na kodekse prakse u smislu članka 56. kako bi dokazali da ispunjavaju obveze utvrđene u stavku 1. ovog članka. Ispunjavanjem europskih usklađenih normi za dobavljače vrijedi pretpostavka sukladnosti u mjeri u kojoj su te obveze obuhvaćene tim normama. Dobavljači UI modelâ opće namjene koji ne poštuju odobreni kodeks prakse ili ne ispunjavaju europsku usklađenu normu moraju dokazati alternativne adekvatne načine usklađivanja kako bi ih ocijenila Komisija.
5. Kako bi se olakšalo usklađivanje s Prilogom XI., a posebno s njegovom točkom 2. podtočkama (d) i (e), Komisija je ovlaštena z donošenje delegiranih akata u skladu s člankom 97. kako bi detaljno opisala metodologije mjerenja i izračuna u cilju omogućavanja usporedive i provjerljive dokumentacije.
6. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 97. stavkom 2. radi izmjene priloga XI. i XII. s obzirom na tehnološki razvoj.
7. Sa svim informacijama ili dokumentacijom koji se pribave u skladu s ovim člankom, uključujući poslovne tajne, postupi se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 54.

Ovlašteni zastupnici dobavljača UI modelâ opće namjene

1. Prije stavljanja UI modelâ opće namjene na tržište Unije dobavljači s poslovnim nastanom u trećim zemljama pisanim ovlaštenjem imenuju ovlaštenog zastupnika s poslovnim nastanom Uniji.

2. Dobavljač omogućuje svojem ovlaštenom zastupniku da obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača.
3. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje je dobio od dobavljača. On dostavlja primjerak ovlaštenja Uredu za umjetnu inteligenciju na njegov zahtjev, na jednom od službenih jezika institucija Unije. Za potrebe ove Uredbe ovlaštenjem se ovlaštenom zastupniku daje ovlast da obavlja sljedeće zadaće:
 - (a) provjerava je li tehnička dokumentacija iz Priloga XI. sastavljena i je li dobavljač ispunio sve obveze iz članka 53. i, ako je primjenjivo, članka 55.;
 - (b) drži primjerak tehničke dokumentacije iz Priloga XI. na raspolaganju Uredu za umjetnu inteligenciju i nacionalnim nadležnim tijelima tijekom razdoblja od deset godina nakon stavljanja UI modela opće namjene na tržište i čuva kontaktne podatke dobavljača koji je imenovao ovlaštenog zastupnika;
 - (c) Uredu za umjetnu inteligenciju na obrazloženi zahtjev dostavlja sve informacije i dokumentaciju, uključujući one iz točke (b), koji su potrebni za dokazivanje ispunjavanja obveza iz ovog poglavlja;
 - (d) na obrazloženi zahtjev surađuje s Uredom za umjetnu inteligenciju i nadležnim tijelima u svim mjerama koje oni poduzimaju u vezi s UI modelom opće namjene, među ostalim onda kada je model integriran u UI sustave koji se stavljaju na tržište ili u upotrebu u Uniji.

4. Ovlaštenjem se ovlaštenog zastupnika ovlašćuje da, uz dobavljača ili umjesto dobavljaču, bude osoba kojoj se obraćaju Ured za umjetnu inteligenciju ili nadležna tijela u vezi sa svim pitanjima povezanim s osiguravanjem usklađenosti s ovom Uredbom.
5. Ovlašteni zastupnik ukida ovlaštenje ako smatra ili ima razloga smatrati da dobavljač postupa protivno svojim obvezama na temelju ove Uredbe. U tom slučaju ovlašteni zastupnik o ukidanju ovlaštenja i razlozima za ukidanje ujedno odmah obavješćuje Ured za umjetnu inteligenciju.
6. Obveza utvrđena u ovom članku ne primjenjuje se na dobavljače UI modela opće namjene koji se objavljuju na temelju besplatne licencije otvorenog koda koja omogućuje pristup modelu te njegovu upotrebu, izmjenu i distribuciju i čiji su parametri, uključujući težinske faktore, informacije o arhitekturi modela te informacije o upotrebi modela, javno dostupni, osim ako UI modeli opće namjene predstavljaju sistemske rizike.

ODJELJAK 3.
OBVEZE DOBAVLJAČA UI MODELÂ OPĆE NAMJENE
SA SISTEMSKIM RIZIKOM

Članak 55.

Obveze dobavljača UI modelâ opće namjene sa sistemskim rizikom

1. Uz obveze navedene u člancima 53. i 54. dobavljači UI modelâ opće namjene sa sistemskim rizikom:
 - (a) provode evaluaciju modela u skladu sa standardiziranim protokolima i alatima koji odražavaju najnovija dostignuća, uključujući provođenje i dokumentiranje neprijateljskog testiranja modela radi utvrđivanja i smanjivanja sistemskog rizika;
 - (b) procjenjuju i smanjuju moguće sistemske rizike na razini Unije, uključujući njihove izvore, koji mogu proizići iz razvoja, stavljanja na tržište ili korištenja UI modelâ opće namjene sa sistemskim rizikom;
 - (c) prate, dokumentiraju i bez nepotrebne odgode dostavljaju Uredu za umjetnu inteligenciju i, prema potrebi, nacionalnim nadležnim tijelima, relevantne informacije o ozbiljnim incidentima i mogućim korektivnim mjerama za njihovo rješavanje;
 - (d) osiguravaju odgovarajuću razinu kibernetičkosigurnosne zaštite UI modela opće namjene sa sistemskim rizikom i fizičke infrastrukture tog modela.

2. Dobavljači UI modelâ opće namjene sa sistemskim rizikom mogu se do objave usklađene norme osloniti na kodekse prakse u smislu članka 56. kako bi dokazali da ispunjavaju obveze utvrđene u stavku 1. ovog članka. Ispunjavanjem europskih usklađenih normi za dobavljače vrijedi pretpostavka sukladnosti u mjeri u kojoj su te obveze obuhvaćene tim normama. Dobavljači UI modelâ opće namjene sa sistemskim rizikom koji ne poštuju odobreni kodeksa prakse ili ne ispunjavaju europsku usklađenu normu moraju dokazati alternativne adekvatne načine usklađivanja kako bi ih procijenila Komisija.
3. Sa svim informacijama ili dokumentacijom koji se pribave na temelju ovog članka, uključujući poslovne tajne, postupaju se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

ODJELJAK 4.

KODEKSI PRAKSE

Članak 56.

Kodeksi prakse

1. Ured za umjetnu inteligenciju potiče i olakšava izradu kodeksâ prakse na razini Unije kako bi se doprinijelo pravilnoj primjeni ove Uredbe, uzimajući u obzir međunarodne pristupe.

2. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju nastoje osigurati da kodeksi prakse obuhvaćaju barem obveze iz članaka 53. i 55., uključujući sljedeća pitanja:
- (a) sredstva kojima se osigurava da se informacije iz članka 53. stavka 1. točaka (a) i (b) ažuriraju s obzirom na tržišni i tehnološki razvoj;
 - (b) odgovarajuću razinu detaljnosti sažetka o sadržaju upotrijebljenom za treniranje;
 - (c) utvrđivanje vrste i prirode sistemskih rizika na razini Unije, uključujući, prema potrebi, njihove izvore;
 - (d) mjere, postupke i modalitete za procjenu sistemskih rizika i upravljanje sistemskim rizicima na razini Unije, uključujući dokumentaciju o njima, koji su razmjerni rizicima i kojima se uzimaju u obzir ozbiljnost i vjerojatnost tih rizika te posebni izazovi uklanjanja tih rizika s obzirom na moguće načine na koje se takvi rizici mogu pojaviti i materijalizirati duž vrijednosnog lanca umjetne inteligencije.
3. Ured za umjetnu inteligenciju može pozvati sve dobavljače UI modelâ opće namjene, kao i relevantna nacionalna nadležna tijela, da sudjeluju u izradi kodeksâ prakse. Taj proces mogu poduprijeti organizacije civilnog društva, industrija, akademska zajednica i drugi relevantni dionici, poput dobavljača niže u lancu opskrbe i neovisnih stručnjaka.

4. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju nastoje osigurati da se u kodeksima prakse jasno utvrde njihovi specifični ciljevi i da sadržavaju obveze ili mjere, prema potrebi uključujući ključne pokazatelje uspješnosti, za osiguravanje postizanja tih ciljeva, te da se u njima na odgovarajući način uzimaju u obzir potrebe i interesi svih zainteresiranih strana, među ostalim uključenih osoba, na razini Unije.
5. Ured za umjetnu inteligenciju nastoji osigurati da sudionici kodeksâ prakse redovito izvješćuju Ured za umjetnu inteligenciju o provedbi obveza i poduzetim mjerama te njihovim rezultatima, među ostalim u odnosu na ključne pokazatelje uspješnosti, prema potrebi. Ključni pokazatelji uspješnosti i obveze izvješćivanja moraju odražavati razlike u veličini i kapacitetu među različitim sudionicima.
6. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju redovito prate i ocjenjuju ostvarivanje ciljeva kodeksâ prakse od strane sudionika i njihov doprinos pravilnoj primjeni ove Uredbe. Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju ocjenjuju obuhvaćaju li kodeksi prakse obveze iz članaka 53. i 55., te redovito prate i evaluiraju postizanje njihovih ciljeva. Objavljuju svoju ocjenu adekvatnosti kodeksâ prakse.

Komisija može provedbenim aktom odobriti kodeks prakse i učiniti ga općenito valjanim u Uniji. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.

7. Ured za umjetnu inteligenciju može pozvati sve dobavljače UI modelâ opće namjene da poštuju kodekse prakse. Za dobavljače UI modela opće namjene koji ne predstavljaju sistemske rizike to poštovanje može se ograničiti na obveze iz članka 53., osim ako izričito izraze interes da se pridruže cijelom kodeksu.
8. Ured za umjetnu inteligenciju prema potrebi također potiče i olakšava preispitivanje i prilagodbu kodeksâ prakse, posebno s obzirom na nove norme. Ured za umjetnu inteligenciju pomaže u ocjenjivanju dostupnih normi.
9. Kodeksi prakse moraju biti spremni najkasnije do ... [devet mjeseci od datuma stupanja na snagu ove Uredbe]. Ured za umjetnu inteligenciju poduzima potrebne korake, uključujući pozivanje dobavljača u skladu sa stavkom 7.

Ako do ... [12 mjeseci od datuma stupanja na snagu ove Uredbe] kodeks prakse ne može biti dovršen ili ako Ured za umjetnu inteligenciju nakon ocjenjivanja na temelju stavka 6. ovog članka smatra da kodeks prakse nije adekvatan, Komisija može provedbenim aktima propisati zajednička pravila za provedbu obveza iz članaka 53. i 55., među ostalim u pogledu pitanja iz stavka 2. ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

Poglavlje VI.

Mjere za potporu inovacijama

Članak 57.

Regulatorna izolirana okruženja za umjetnu inteligenciju

1. Države članice osiguravaju da njihova nadležna tijela uspostave barem jedno regulatorno izolirano okruženje za umjetnu inteligenciju na nacionalnoj razini, koje mora biti operativno do ... [24 mjeseca od datuma stupanja na snagu ove Uredbe]. To izolirano okruženje može se uspostaviti i zajedno s nadležnim tijelima drugih država članica. Komisija može pružiti tehničku potporu, savjete i alate za uspostavu i rad regulatornih izoliranih okruženja za umjetnu inteligenciju.

Obveza iz prvog podstavka može se ispuniti i sudjelovanjem u postojećem izoliranom okruženju ako se tim sudjelovanjem osigurava jednakovrijedna razina nacionalne pokrivenosti za države članice sudionice.

2. Mogu se uspostaviti i dodatna regulatorna izolirana okruženja za umjetnu inteligenciju na regionalnoj ili lokalnoj razini ili se ona mogu uspostaviti zajedno s nadležnim tijelima drugih država članica.
3. Europski nadzornik za zaštitu podataka također može uspostaviti regulatorno izolirano okruženje za umjetnu inteligenciju za institucije, tijela, urede i agencije Unije te može izvršavati uloge i zadaće nacionalnih nadležnih tijela u skladu s ovim poglavljem.

4. Države članice osiguravaju da nadležna tijela iz stavaka 1. i 2. dodijele dostatna sredstva za djelotvorno i pravodobno usklađivanje s ovim člankom. Nacionalna nadležna tijela prema potrebi surađuju s drugim relevantnim tijelima i mogu dopustiti sudjelovanje drugih aktera iz ekosustava umjetne inteligencije. Ovaj članak ne utječe na druga regulatorna izolirana okruženja uspostavljena na temelju prava Unije ili nacionalnog prava. Države članice osiguravaju odgovarajuću razinu suradnje između tijela koja nadziru ta druga izolirana okruženja i nacionalnih nadležnih tijela.
5. Regulatorna izolirana okruženja za umjetnu inteligenciju uspostavljena na temelju stavka 1. pružaju kontrolirano okruženje koje potiče inovacije i olakšava razvoj, treniranje, testiranje i validaciju inovativnih UI sustava tijekom ograničenog razdoblja prije njihova stavljanja na tržište ili u upotrebu u skladu s posebnim planom izoliranog okruženja dogovorenim između dobavljača ili potencijalnih dobavljača i nadležnog tijela. Takva izolirana okruženja mogu uključivati testiranje u stvarnim uvjetima pod nadzorom u izoliranom okruženju.
6. Nadležna tijela prema potrebi pružaju smjernice, nadzor i potporu u regulatornom izoliranom okruženju za umjetnu inteligenciju radi utvrđivanja rizika, posebno za temeljna prava, zdravlje i sigurnost, te radi utvrđivanja testiranja, mjera ublažavanja i njihove djelotvornosti u odnosu na obveze i zahtjeve iz ove Uredbe i, prema potrebi, iz drugog prava Unije i nacionalnog prava čije se ispunjavanje nadzire u izoliranom okruženju.
7. Nadležna tijela dobavljačima i potencijalnim dobavljačima koji sudjeluju u regulatornom izoliranom okruženju za umjetnu inteligenciju pružaju smjernice o regulatornim očekivanjima i načinu ispunjavanja zahtjeva i obveza utvrđenih u ovoj Uredbi.

Na zahtjev dobavljača ili potencijalnog dobavljača UI sustava nadležno tijelo dostavlja pisani dokaz o aktivnostima koje su uspješno provedene u izoliranom okruženju. Nadležno tijelo dostavlja i završno izvješće koje sadržava pojedinosti o aktivnostima provedenima u izoliranom okruženju te povezanim rezultatima i ishodima učenja. Dobavljači mogu takvu dokumentaciju upotrijebiti kako bi dokazali svoju usklađenost s ovom Uredbom putem postupka ocjenjivanja sukladnosti ili relevantnih aktivnosti nadzora tržišta. U tom pogledu tijela za nadzor tržišta i prijavljena tijela pozitivno uzimaju u obzir završna izvješća i pisane dokaze koje je dostavilo nacionalno nadležno tijelo kako bi se u razumnoj mjeri ubrzali postupci ocjenjivanja sukladnosti.

8. Podložno odredbama o povjerljivosti iz članka 78. i uz suglasnost dobavljača ili potencijalnog dobavljača, Komisija i Vijeće za umjetnu inteligenciju ovlašteni su pristupiti završnim izvješćima te ih prema potrebi uzimaju u obzir pri izvršavanju svojih zadaća na temelju ove Uredbe. Ako se i dobavljač odnosno potencijalni dobavljač i nacionalno nadležno tijelo o tome izričito dogovore, završno izvješće može se objaviti na jedinstvenoj informacijskoj platformi iz ovog članka.
9. Svrha uspostave regulatornih izoliranih okruženja za umjetnu inteligenciju doprinošenje je sljedećim ciljevima:
 - (a) unapređivanju pravne sigurnosti radi postizanja regulatorne usklađenosti s ovom Uredbom ili, prema potrebi, drugim primjenjivim pravom Unije i nacionalnim pravom;
 - (b) podupiranju razmjene primjera najbolje prakse putem suradnje s tijelima uključenima u regulatorno izolirano okruženje za umjetnu inteligenciju;

- (c) poticanju inovacija i konkurentnosti te olakšavanju razvoja ekosustava umjetne inteligencije;
 - (d) doprinosenju regulatornom učenju utemeljenom na dokazima;
 - (e) olakšavanju i ubrzavanju pristupa UI sustava tržištu Unije, posebno ako su njihovi dobavljači MSP-ovi, uključujući start-up poduzeća.
10. Nacionalna nadležna tijela osiguravaju da, ako inovativni UI sustavi obuhvaćaju obradu osobnih podataka ili su na neki drugi način obuhvaćeni nadzorom drugih nacionalnih tijela ili nadležnih tijela koja pružaju ili podržavaju pristup podacima, nacionalna tijela za zaštitu podataka i ta druga nacionalna ili nadležna tijela budu uključena u rad regulatornog izoliranog okruženja za umjetnu inteligenciju i uključena u nadzor nad tim aspektima u okviru svojih zadaća i ovlasti.
11. Regulatorna izolirana okruženja za umjetnu inteligenciju ne utječu na nadzorne ili korektivne ovlasti nadležnih tijela koja nadziru izolirana okruženja, među ostalim na regionalnoj ili lokalnoj razini. Ako se tijekom razvoja i testiranja takvih UI sustava uoče znatni rizici za zdravlje, sigurnost i temeljna prava, ti se rizici moraju adekvatno ublažiti. Nacionalna nadležna tijela ovlaštena su privremeno ili trajno suspendirati postupak testiranja ili sudjelovanje u izoliranom okruženju ako rizike nije moguće djelotvorno ublažiti, a o takvoj odluci obavješćuju Ured za umjetnu inteligenciju. Nacionalna nadležna tijela izvršavaju svoje nadzorne ovlasti u granicama relevantnog prava i primjenjuju svoje diskrecijske ovlasti pri provedbi pravnih odredaba u odnosu na određeni projekt u regulatornom izoliranom okruženju za umjetnu inteligenciju, s ciljem podupiranja inovacija u području umjetne inteligencije u Uniji.

12. Dobavljači i potencijalni dobavljači koji sudjeluju u regulatornom izoliranom okruženju za umjetnu inteligenciju i dalje su na temelju primjenjivog prava Unije o odgovornosti i nacionalnog prava o odgovornosti odgovorni za svu štetu nanесenu trećim stranama koja je posljedica eksperimentiranja u izoliranom okruženju. Međutim, ako potencijalni dobavljači poštuju posebni plan i uvjete svojeg sudjelovanja te u dobroj vjeri slijede smjernice nacionalnog nadležnog tijela, tijela ne izriču upravne novčane kazne zbog povrede ove Uredbe. Ako su druga nadležna tijela koja su odgovorna za drugo pravo Unije i nacionalno pravo bila aktivno uključena u nadzor nad UI sustavom u izoliranom okruženju i dala smjernice u pogledu usklađivanja, ne izriču se upravne novčane kazne u vezi s tim pravom.
13. Regulatorna izolirana okruženja za umjetnu inteligenciju dizajniraju se i realiziraju na takav način da se njima, ako je to relevantno, olakšava prekogranična suradnja među nacionalnim nadležnim tijelima.
14. Nacionalna nadležna tijela koordiniraju svoje aktivnosti i surađuju u okviru Vijeća za umjetnu inteligenciju.
15. Nacionalna nadležna tijela obavješćuju Ured za umjetnu inteligenciju i Vijeće za umjetnu inteligenciju o uspostavi izoliranog okruženja i mogu od njih zatražiti potporu i smjernice. Ured za umjetnu inteligenciju objavljuje popis planiranih i postojećih izoliranih okruženja i ažurira ga kako bi se potaknula veća interakcija u regulatornim izoliranim okruženjima za umjetnu inteligenciju i prekogranična suradnja.

16. Nacionalna nadležna tijela podnose godišnja izvješća Uredu za umjetnu inteligenciju i Vijeću za umjetnu inteligenciju, počevši godinu dana nakon uspostave regulatornog izoliranog okruženja za umjetnu inteligenciju i svake godine nakon toga do njegove obustave, te završno izvješće. U tim se izvješćima navode informacije o napretku i rezultatima provedbe tih izoliranih okruženja, uključujući primjere najbolje prakse, incidente, stečena iskustva i preporuke o strukturi tih izoliranih okruženja te, prema potrebi, o primjeni i mogućoj reviziji ove Uredbe, uključujući njezine delegirane akte i provedbene akte, te o primjeni drugog prava Unije koju nadležna tijela nadziru u relevantnom izoliranom okruženju. Nacionalna nadležna tijela ta godišnja izvješća ili njihove sažetke stavljaju na raspolaganje javnosti na internetu. Komisija ta godišnja izvješća prema potrebi uzima u obzir pri izvršavanju svojih zadaća na temelju ove Uredbe.
17. Komisija izrađuje jedinstveno, namjensko sučelje koje sadržava sve relevantne informacije povezane s izoliranim okruženjima za umjetnu inteligenciju kako bi se dionicima omogućilo da ostvare interakciju s regulatornim izoliranim okruženjima za umjetnu inteligenciju, podnesu upite nadležnim tijelima i zatraže neobvezujuće smjernice u vezi sa sukladnošću inovativnih proizvoda, usluga i poslovnih modela u koje su ugrađene tehnologije umjetne inteligencije, u skladu s člankom 62. stavkom 1. točkom (c). Komisija se prema potrebi proaktivno koordinira s nacionalnim nadležnim tijelima.

Članak 58.

Detaljni aranžmani za regulatorna izolirana okruženja za umjetnu inteligenciju i njihovo funkcioniranje

1. Kako bi se u Uniji izbjegla fragmentacija, Komisija donosi provedbene akte o utvrđivanju detaljnih aranžmana za uspostavu, razvoj, provedbu, rad i nadzor regulatornih izoliranih okruženja za umjetnu inteligenciju. Ti provedbeni akti sadržavaju zajednička načela o sljedećim pitanjima:

- (a) kriterijima prihvatljivosti i odabira za sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju;
- (b) postupcima za primjenu regulatornog izoliranog okruženja za umjetnu inteligenciju, sudjelovanje u njemu, njegovo praćenje, izlazak iz njega i njegovu obustavu, što uključuje plan izoliranog okruženja i završno izvješće;
- (c) uvjetima koji se primjenjuju na sudionike.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

2. Provedbenim aktima iz stavka 1. osigurava se sljedeće:

- (a) regulatorna izolirana okruženja za umjetnu inteligenciju otvorena su svim dobavljačima ili potencijalnim dobavljačima UI sustava koji ispunjava kriterije prihvatljivosti i odabira, koji su transparentni i pošteni, a nacionalna nadležna tijela obavješćuju podnositelje zahtjeva o svojoj odluci u roku od tri mjeseca od podnošenja zahtjeva;

- (b) regulatorna izolirana okruženja za umjetnu inteligenciju omogućuju širok i jednak pristup te drže korak s potražnjom za sudjelovanjem; dobavljači i potencijalni dobavljači također mogu podnijeti zahtjeve u partnerstvu sa subjektima koji uvode sustav i drugim relevantnim trećim stranama;
- (c) detaljnim aranžmanima i uvjetima za regulatorna izolirana okruženja za umjetnu inteligenciju u najvećoj se mogućoj mjeri podupire fleksibilnost nacionalnih nadležnih tijela u uspostavi regulatornih izoliranih okruženja za umjetnu inteligenciju i upravljanju njima;
- (d) pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju besplatan je za MSP-ove, uključujući *start-up* poduzeća, ne dovodeći u pitanje izvanredne troškove čiju naknadu na pravedan i razmjeran način mogu zatražiti nacionalna nadležna tijela;
- (e) dobavljačima i potencijalnim dobavljačima olakšavaju, s pomoću ishoda učenja regulatornih izoliranih okruženja za umjetnu inteligenciju, ispunjavanje obveza u pogledu ocjenjivanja sukladnosti na temelju ove Uredbe i dobrovoljnu primjenu kodeksa ponašanja iz članka 95.;
- (f) kako bi se omogućila i olakšala suradnja s javnim sektorom i s privatnim sektorom, regulatorna izolirana okruženja za umjetnu inteligenciju olakšavaju sudjelovanje drugih relevantnih aktera iz ekosustava umjetne inteligencije, kao što su prijavljena tijela i organizacije za normizaciju, MSP-ovi, uključujući *start-up* poduzeća, poduzeća, inovatori, objekti za testiranje i eksperimentiranje, laboratoriji za istraživanja i eksperimentiranje, europski centri za digitalne inovacije, centri izvrsnosti i pojedinačni istraživači;

- (g) postupci, procesi i administrativni uvjeti za podnošenje zahtjeva, odabir, sudjelovanje i izlazak iz regulatornog izoliranog okruženja za umjetnu inteligenciju jednostavni su, lako razumljivi i jasno priopćeni kako bi se olakšalo sudjelovanje MSP-ova, uključujući *start-up* poduzeća, s ograničenim pravnim i administrativnim kapacitetima i pojednostavnjeni su u cijeloj Uniji kako bi se izbjegla rascjepkanost i kako bi se sudjelovanje u regulatornom izoliranom okruženju koje je uspostavila država članica ili Europski nadzornik za zaštitu podataka uzajamno i ujednačeno priznavalo te imalo iste pravne učinke u cijeloj Uniji;
- (h) sudjelovanje u regulatornom izoliranom okruženju za umjetnu inteligenciju ograničeno je na razdoblje koje je primjereno složenosti i opsegu projekta i koje može produljiti nacionalno nadležno tijelo;
- (i) regulatorna izolirana okruženja za umjetnu inteligenciju olakšavaju razvoj alata i infrastrukture za testiranje, utvrđivanje referentnih vrijednosti, ocjenjivanje i objašnjavanje dimenzija UI sustava koje su relevantne za regulatorno učenje, poput točnosti, otpornosti i kibernetičke sigurnosti, kao i mjera za ublažavanje rizika za temeljna prava i društvo u cjelini.

3. Potencijalne dobavljače u regulatornim izoliranim okruženjima za umjetnu inteligenciju, posebno MSP-ove i *start-up* poduzeća, prema potrebi se usmjerava na usluge prije uvođenja, kao što su smjernice o provedbi ove Uredbe, na druge usluge s dodanom vrijednošću, kao što su pomoć u vezi s dokumentima o normizaciji i certifikacijom, na objekte za testiranje i eksperimentiranje, europske centre za digitalne inovacije i centre izvrsnosti.

4. Kada nacionalna nadležna tijela razmatraju izdavanje odobrenja za testiranje u stvarnim uvjetima koje se nadzire u okviru regulatornog izoliranog okruženja za umjetnu inteligenciju koje treba uspostaviti na temelju ovog članka, sa sudionicima izričito dogovaraju uvjete tog testiranja, a posebno odgovarajuće zaštitne mjere u cilju zaštite temeljnih prava, zdravlja i sigurnosti. Prema potrebi surađuju s drugim nacionalnim nadležnim tijelima kako bi se osigurala dosljedna praksa u cijeloj Uniji.

Članak 59.

Daljnja obrada osobnih podataka za razvoj određenih UI sustava u javnom interesu u regulatornom izoliranom okruženju za umjetnu inteligenciju

1. U regulatornom izoliranom okruženju za umjetnu inteligenciju osobni podaci koji su zakonito prikupljeni u druge svrhe mogu se obrađivati samo u svrhu razvoja, treniranja i testiranja određenih UI sustava u izoliranom okruženju ako su ispunjeni svi sljedeći uvjeti:
 - (a) UI sustave razvija tijelo javne vlasti ili druga fizička ili pravna osoba u svrhu zaštite znatnog javnog interesa, u jednom ili više sljedećih područja:
 - i. javna sigurnost i javno zdravlje, uključujući otkrivanje, dijagnosticiranje, prevenciju, kontrolu i liječenje bolesti te unapređivanje zdravstvenih sustava;
 - ii. visoka razina zaštite i poboljšanje kvalitete okoliša, zaštita bioraznolikosti, zaštita od onečišćenja, mjere zelene tranzicije, mjere za ublažavanje klimatskih promjena i prilagodbu njima;

- iii. energetska održivost;
 - iv. sigurnost i otpornost prometnih sustava i mobilnosti, kritične infrastrukture i mreža;
 - v. učinkovitost i kvaliteta javne uprave i javnih usluga;
- (b) podaci koji se obrađuju potrebni su za ispunjavanje jednog ili više zahtjeva iz poglavlja III. odjeljka 2. ako se ti zahtjevi ne mogu djelotvorno ispuniti obradom anonimiziranih, sintetičkih ili drugih neosobnih podataka;
- (c) postoje djelotvorni mehanizmi praćenja kojima se može utvrditi mogu li se tijekom eksperimentiranja u izoliranom okruženju pojaviti veliki rizici za prava i slobode ispitanikâ, kako je navedeno u članku 35. Uredbe (EU) 2016/679 i u članku 39. Uredbe (EU) 2018/1725, kao i mehanizmi za odgovor kojima se ti rizici mogu brzo ublažiti, a obrada prema potrebi zaustaviti;
- (d) osobni podaci koji se obrađuju u izoliranom okruženju nalaze se u funkcionalno odvojenom, izoliranom i zaštićenom okruženju za obradu podataka pod kontrolom potencijalnog dobavljača i samo ovlaštene osobe imaju pristup tim podacima;
- (e) dobavljači mogu dalje dijeliti izvorno prikupljene podatke samo u skladu s pravom Unije o zaštiti podataka; osobni podaci nastali u izoliranom okruženju ne mogu se dijeliti izvan izoliranog okruženja;

- (f) obrada osobnih podataka u kontekstu izoliranog okruženja ne smije dovesti do mjera ili odluka koje utječu na ispitanike niti smije utjecati na ostvarivanje njihovih prava utvrđenih u pravu Unije o zaštiti osobnih podataka;
- (g) osobni podaci koji se obrađuju u kontekstu izoliranog okruženja zaštićeni su odgovarajućim tehničkim i organizacijskim mjerama i brišu se nakon okončanja sudjelovanja u izoliranom okruženju ili isteka razdoblja čuvanja osobnih podataka;
- (h) evidencija obrade osobnih podataka u kontekstu izoliranog okruženja čuva se za vrijeme sudjelovanja u izoliranom okruženju, osim ako je pravom Unije ili nacionalnim pravom predviđeno drukčije;
- (i) u sklopu tehničke dokumentacije iz Priloga IV. zajedno s rezultatima testiranja čuva se potpun i detaljan opis procesa i obrazloženja treniranja, testiranja i validacije dotičnog UI sustava;
- (j) na internetskim stranicama nadležnih tijela objavljuju se kratak sažetak projekta umjetne inteligencije razvijenog u izoliranom okruženju te njegovi ciljevi i očekivani rezultati; ta obveza ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor državne granice, tijela za imigraciju ili tijela za azil.

2. U svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija, što uključuje zaštitu od prijetnji javnoj sigurnosti i sprečavanje tih prijetnji, pod kontrolom i odgovornošću tijela kaznenog progona, obrada osobnih podataka u regulatornim izoliranim okruženjima za umjetnu inteligenciju temelji se na posebnom pravu Unije ili nacionalnom pravu i podliježe istim kumulativnim uvjetima iz stavka 1.
3. Stavkom 1. ne dovodi se u pitanje pravo Unije ili nacionalno pravo kojim se isključuje obrada osobnih podataka u svrhe koje nisu izričito navedene u tom pravu, kao ni pravo Unije ili nacionalno pravo kojim se utvrđuje osnova za obradu osobnih podataka koja je potrebna u svrhu razvoja, testiranja ili treniranja inovativnih UI sustava ili bilo koja druga pravna osnova, u skladu s pravom Unije o zaštiti osobnih podataka.

Članak 60.

Testiranje visokorizičnih UI sustava u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju

1. Testiranje visokorizičnih UI sustava u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju mogu provoditi dobavljači ili potencijalni dobavljači visokorizičnih UI sustava iz Priloga III. u skladu s ovim člankom i planom testiranja u stvarnim uvjetima iz ovog članka, ne dovodeći u pitanje zabrane na temelju članka 5.

Komisija provedbenim aktima utvrđuje pojedinosti plana testiranja u stvarnim uvjetima. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

Ovim se stavkom ne dovodi u pitanje pravo Unije ili nacionalno pravo o testiranju u stvarnim uvjetima visokorizičnih UI sustava povezanih s proizvodima obuhvaćenima zakonodavstvom Unije o usklađivanju navedenim u Prilogu I.

2. Dobavljači ili potencijalni dobavljači mogu u bilo kojem trenutku prije stavljanja UI sustava na tržište ili u upotrebu provesti testiranje visokorizičnih UI sustava iz Priloga III. u stvarnim uvjetima, samostalno ili u partnerstvu s jednim ili više subjekata koji uvode sustav ili potencijalnih subjekata koji uvode sustav.
3. Testiranjem visokorizičnih UI sustava u stvarnim uvjetima na temelju ovog članka ne dovodi se u pitanje etičko preispitivanje koje se zahtijeva pravom Unije ili nacionalnim pravom.
4. Dobavljači ili potencijalni dobavljači testiranje u stvarnim uvjetima mogu provesti samo ako su ispunjeni svi sljedeći uvjeti:
 - (a) dobavljač ili potencijalni dobavljač izradio je plan testiranja u stvarnim uvjetima i dostavio ga tijelu za nadzor tržišta u državi članici u kojoj će se provoditi testiranje u stvarnim uvjetima;
 - (b) tijelo za nadzor tržišta u državi članici u kojoj će se provoditi testiranje u stvarnim uvjetima odobrilo je testiranje u stvarnim uvjetima i plan testiranja u stvarnim uvjetima; ako tijelo za nadzor tržišta ne odgovori u roku od 30 dana, smatra se da su testiranje u stvarnim uvjetima i plan testiranja u stvarnim uvjetima odobreni; ako nacionalnim pravom nije predviđeno prešutno odobrenje, testiranje u stvarnim uvjetima i dalje podliježe odobrenju;

- (c) dobavljač ili potencijalni dobavljač, uz iznimku dobavljača ili potencijalnih dobavljača visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III. u područjima kaznenog progona, migracija, azila i upravljanja nadzorom državne granice i visokorizičnih UI sustava iz točke 2. Priloga III., registrirao je testiranje u stvarnim uvjetima u skladu s člankom 71. stavkom 4. pri čemu je naveo jedinstveni identifikacijski broj na razini Unije i informacije iz Priloga IX.; dobavljač ili potencijalni dobavljač visokorizičnih UI sustava iz točaka 1., 6. i 7. Priloga III. u područjima kaznenog progona, migracija, azila i upravljanja nadzorom državne granice registrirao je testiranje u stvarnim uvjetima u dijelu baze podataka EU-a koji nije javno dostupan u skladu s člankom 49. stavkom 4. točkom (d) pri čemu je naveo jedinstveni identifikacijski broj na razini Unije i informacije sadržane u njemu; dobavljač ili potencijalni dobavljač visokorizičnih UI sustava iz točke 2. Priloga III. registrirao je testiranje u stvarnim uvjetima u skladu s člankom 49. stavkom 5.;
- (d) dobavljač ili potencijalni dobavljač koji provodi testiranje u stvarnim uvjetima ima poslovni nastan u Uniji ili je imenovao pravnog zastupnika s poslovnim nastanom u Uniji;
- (e) podaci koji se prikupljaju i obrađuju u svrhu testiranja u stvarnim uvjetima prenose se trećim zemljama samo pod uvjetom da se provode odgovarajuće i primjenjive zaštitne mjere na temelju prava Unije;

- (f) testiranje u stvarnim uvjetima ne traje dulje nego što je potrebno za postizanje njegovih ciljeva, a u svakom slučaju ne dulje od šest mjeseci, što se može produžiti za dodatno razdoblje od šest mjeseci, pod uvjetom da dobavljač ili potencijalni dobavljač o tome prethodno obavijesti tijelo za nadzor tržišta, čemu prilaže objašnjenje potrebe za takvim produženjem;
- (g) ispitanici koji sudjeluju u testiranju u stvarnim uvjetima koji zbog svoje dobi ili invaliditeta pripadaju skupinama ranjivih osoba primjereno su zaštićeni;
- (h) ako dobavljač ili potencijalni dobavljač organizira testiranje u stvarnim uvjetima u suradnji s jednim ili više subjekata koji uvode sustav ili potencijalnih subjekata koji uvode sustav, korisnici su obaviješteni o svim aspektima testiranja koji su relevantni za njihovu odluku o sudjelovanju i dane su im relevantne upute za korištenje UI sustava iz članka 13.; dobavljač ili potencijalni dobavljač i subjekt koji uvodi sustav ili potencijalni subjekt koji uvodi sustav sklapaju sporazum kojim se utvrđuju njihove uloge i odgovornosti kako bi se osigurala usklađenost s odredbama za testiranje u stvarnim uvjetima na temelju ove Uredbe i na temelju drugog primjenjivog prava Unije i nacionalnog prava;
- (i) ispitanici koji sudjeluju u testiranju u stvarnim uvjetima dali su informirani pristanak u skladu s člankom 61. ili, u slučaju kaznenog progona, ako bi traženje informiranog pristanka spriječilo testiranje UI sustava, sâmo testiranje i ishod testiranja u stvarnim uvjetima ne smiju imati negativan učinak na ispitanike, a njihovi osobni podaci brišu se nakon provedbe testiranja;

- (j) testiranje u stvarnim uvjetima djelotvorno nadzire dobavljač ili potencijalni dobavljač, kao i subjekti koji uvode sustav ili potencijalni subjekti koji uvode sustav, posredstvom osoba koje imaju odgovarajuće kvalifikacije u relevantnom području te koje imaju potrebne kapacitete, osposobljavanje i ovlasti za obavljanje svojih zadaća;
- (k) predviđanja, preporuke ili odluke UI sustava mogu se djelotvorno poništiti i zanemariti.

- 5. Svi ispitanici koji sudjeluju u testiranju u stvarnim uvjetima ili, ovisno o slučaju, njihov zakonito imenovani zastupnik, mogu se u bilo kojem trenutku povući iz testiranja povlačenjem svojeg informiranog pristanka, a da to za njih nema nikakve negativne posljedice i da pritom ne moraju pružiti nikakvo obrazloženje, te mogu zatražiti da se njihovi osobni podaci odmah i trajno izbrišu. Povlačenje informiranog pristanka ne utječe na već provedene aktivnosti.
- 6. U skladu s člankom 75. države članice svojim tijelima za nadzor tržišta dodjeljuju ovlasti da od dobavljača i potencijalnih dobavljača zatraže informacije, da provode nenajavljene inspekcije na daljinu ili na licu mjesta i da obavljaju provjere provedbe testiranja u stvarnim uvjetima i povezanih visokorizičnih UI sustava. Tijela za nadzor tržišta koriste te ovlasti kako bi osigurala siguran razvoj testiranja u stvarnim uvjetima.

7. Svaki ozbiljan incident utvrđen tijekom testiranja u stvarnim uvjetima mora se prijaviti nacionalnom tijelu za nadzor tržišta u skladu s člankom 73. Dobavljač ili potencijalni dobavljač odmah donosi mjere ublažavanja ili, ako to nije moguće, suspendira testiranje u stvarnim uvjetima dok se takve mjere ublažavanja ne provedu ili ga u suprotnom slučaju obustavlja. Dobavljač ili potencijalni dobavljač uspostavlja postupak za promptni opoziv UI sustava nakon takve obustave testiranja u stvarnim uvjetima.
8. Dobavljači ili potencijalni dobavljači obavješćuju nacionalno tijelo za nadzor tržišta u državi članici u kojoj se će se provoditi testiranje u stvarnim uvjetima o suspenziji ili obustavi testiranja u stvarnim uvjetima i konačnim ishodima.
9. Dobavljač ili potencijalni dobavljač odgovoran je na temelju primjenjivog prava Unije o odgovornosti i nacionalnog prava o odgovornosti za svu štetu prouzročenu tijekom svojeg testiranja u stvarnim uvjetima.

Članak 61.

Informirani pristanak za sudjelovanje u testiranju u stvarnim uvjetima izvan regulatornih izoliranih okruženja za umjetnu inteligenciju

1. Za potrebe testiranja u stvarnim uvjetima na temelju članka 60. od ispitanika koji sudjeluju u testiranju pribavlja se dobrovoljan informirani pristanak prije njihova sudjelovanja u takvom testiranju, a nakon što su s pomoću jezgrovitih, jasnih, relevantnih i razumljivih informacija propisno obaviješteni o sljedećem:
 - (a) prirodi i ciljevima testiranja u stvarnim uvjetima i mogućim neugodnostima koje mogu biti povezane s njihovim sudjelovanjem;
 - (b) uvjetima pod kojima će se provoditi testiranje u stvarnim uvjetima, uključujući očekivano trajanje sudjelovanja ispitanika;
 - (c) njihovim pravima i jamstvima u pogledu sudjelovanja, osobito o njihovu pravu na odbijanje sudjelovanja u testiranju u stvarnim uvjetima i pravu na povlačenje iz njega u bilo kojem trenutku, a da to za njih nema nikakve negativne posljedice i da pritom ne moraju pružiti nikakvo obrazloženje;
 - (d) aranžmanima za podnošenje zahtjeva za poništenje ili zanemarivanje predviđanja, preporuka ili odluka UI sustava;
 - (e) jedinstvenom identifikacijskom broju na razini Unije za testiranje u stvarnim uvjetima, u skladu s člankom 60. stavkom 4. točkom (c) i kontaktnim podacima dobavljača ili njegova pravnog zastupnika od kojeg se mogu dobiti dodatne informacije.

2. Informirani pristanak mora biti datiran i dokumentiran, a primjerak se daje ispitanicima koji sudjeluju u testiranju ili njihovom pravnom zastupniku.

Članak 62.

*Mjere za dobavljače i subjekte koji uvode sustav,
posebno MSP-ove, uključujući start-up poduzeća*

1. Države članice poduzimaju sljedeće mjere:
 - (a) MSP-ovima, uključujući *start-up* poduzeća, koji u Uniji imaju registrirani ured ili podružnicu, daju prioritetni pristup regulatornim izoliranim okruženjima za umjetnu inteligenciju, u onoj mjeri u kojoj ispunjavaju uvjete prihvatljivosti i kriterije odabira; prioritetni pristup ne sprečava druge MSP-ove, uključujući *start-up* poduzeća, koja nisu ona iz ovog stavka, da pristupe regulatornom izoliranom okruženju za umjetnu inteligenciju, pod uvjetom da i oni ispunjavaju uvjete prihvatljivosti i kriterije odabira;
 - (b) organiziraju specifične aktivnosti podizanja svijesti i osposobljavanja o primjeni ove Uredbe, prilagođene potrebama MSP-ova, uključujući *start-up* poduzeća, subjekata koji uvode sustav te, prema potrebi, lokalnih tijela javne vlasti;
 - (c) koriste postojeće namjenske kanale za komunikaciju i prema potrebi uspostavljaju nove kanale za komunikaciju s MSP-ovima, uključujući *start-up* poduzeća, sa subjektima koji uvode sustav, s drugim inovatorima i, prema potrebi, s lokalnim tijelima javne vlasti, radi pružanja savjeta i odgovaranja na upite u vezi s provedbom ove Uredbe, među ostalim u pogledu sudjelovanja u regulatornim izoliranim okruženjima za umjetnu inteligenciju;

- (d) olakšavaju sudjelovanje MSP-ova i drugih relevantnih dionika u procesu razvoja normizacije.
2. Pri određivanju naknada za ocjenjivanje sukladnosti na temelju članka 43. uzimaju se u obzir specifični interesi i potrebe dobavljača koji su MSP-ovi, uključujući *start-up* poduzeća, i te se naknade umanjuju razmjerno njihovoj veličini, veličini tržišta i drugim relevantnim pokazateljima.
3. Ured za umjetnu inteligenciju poduzima sljedeće mjere:
- (a) osigurava standardizirane predloške za područja obuhvaćena ovom Uredbom, kako je navelo Vijeće za umjetnu inteligenciju u svojem zahtjevu;
 - (b) razvija i održava jedinstvenu informacijsku platformu na kojoj se svim operaterima iz cijele Unije pružaju informacije u vezi s ovom Uredbom koje su jednostavne za upotrebu;
 - (c) organizira odgovarajuće komunikacijske kampanje za podizanje svijesti o obvezama koje proizlaze iz ove Uredbe;
 - (d) evaluira i promiče konvergenciju primjera najbolje prakse u postupcima javne nabave u vezi s UI sustavima.

Članak 63.

Odstupanja za specifične operatere

1. Mikropoduzeća u smislu Preporuke 2003/361/EZ mogu na pojednostavnjen način ispuniti određene elemente sustava upravljanja kvalitetom koji se zahtijeva člankom 17. ove Uredbe, pod uvjetom da nemaju partnerska poduzeća ili povezana poduzeća u smislu te preporuke. U tu svrhu Komisija izrađuje smjernice o elementima sustava upravljanja kvalitetom koji se mogu ispuniti na pojednostavnjen način s obzirom na potrebe mikropoduzeća, a da se pritom ne utječe na razinu zaštite ili potrebu za ispunjavanjem zahtjeva u vezi s visokorizičnim UI sustavima.
2. Stavak 1. ovog članka ne smije se tumačiti kao izuzimanje tih operatera od ispunjavanja bilo kojih drugih zahtjeva ili obveza utvrđenih u ovoj Uredbi, uključujući one utvrđene u člancima 9., 10., 11., 12., 13., 14., 15., 72. i 73.

Poglavlje VII.

Upravljanje

ODJELJAK 1.

UPRAVLJANJE NA RAZINI UNIJE

Članak 64.

Ured za umjetnu inteligenciju

1. Komisija putem Ureda za umjetnu inteligenciju razvija stručno znanje i sposobnosti Unije u području umjetne inteligencije.
2. Države članice olakšavaju provedbu zadaća povjerenih Uredu za umjetnu inteligenciju, kako su odražene u ovoj Uredbi.

Članak 65.

Osnivanje i struktura Europskog vijeća za umjetnu inteligenciju

1. Osniva se Europsko vijeće za umjetnu inteligenciju („Vijeće za umjetnu inteligenciju”).

2. Vijeće za umjetnu inteligenciju sastoji se od jednog predstavnika iz svake države članice. Europski nadzornik za zaštitu podataka sudjeluje u njemu kao promatrač. Ured za umjetnu inteligenciju također prisustvuje sastancima Vijeća za umjetnu inteligenciju, bez sudjelovanja u glasovanju. Ovisno o pojedinačnom slučaju, Vijeće za umjetnu inteligenciju na sastanke može pozvati druga nacionalna tijela ili stručnjake i Unijina tijela ili stručnjake ako su pitanja o kojima se raspravlja relevantna za njih.
3. Svakog predstavnika imenuje njegova država članica na razdoblje od tri godine, koje se može jednom produljiti.
4. Države članice osiguravaju da za njihove predstavnike u Vijeću za umjetnu inteligenciju vrijedi sljedeće:
 - (a) posjeduju relevantne kompetencije i ovlasti u svojoj državi članici kako bi aktivno doprinosili ostvarivanju zadaca Vijeća za umjetnu inteligenciju iz članka 66.;
 - (b) određeni su kao jedinstvena kontaktna točka u odnosu na Vijeće za umjetnu inteligenciju i, prema potrebi, uzimajući u obzir potrebe država članica, kao jedinstvena kontaktna točka za dionike;
 - (c) ovlašteni su olakšavati dosljednost i koordinaciju među nacionalnim nadležnim tijelima u svojoj državi članici u pogledu provedbe ove Uredbe, među ostalim prikupljanjem relevantnih podataka i informacija u svrhu ispunjavanja svojih zadaca u Vijeću za umjetnu inteligenciju.
5. Imenovani predstavnici država članica donose poslovnik Vijeća za umjetnu inteligenciju dvotrećinskom većinom. Poslovnikom se osobito utvrđuju postupci za postupak odabira, trajanje mandata i specifikacije zadaća predsjednika, detaljni aranžmani za glasovanje te organizacija aktivnosti Vijeća za umjetnu inteligenciju i aktivnosti njegovih podskupina.

6. Vijeće za umjetnu inteligenciju osniva dvije stalne podskupine kako bi osigurao platformu za suradnju i razmjenu među tijelima za nadzor tržišta i tijelima koja provode prijavljivanje o pitanjima koja se odnose na nadzor tržišta odnosno na prijavljena tijela.

Stalna podskupina za nadzor tržišta trebala bi djelovati kao skupina za administrativnu suradnju (skupina za ADCO) za ovu Uredbu u smislu članka 30. Uredbe (EU) 2019/1020.

Vijeće za umjetnu inteligenciju prema potrebi može osnovati druge stalne ili privremene podskupine za razmatranje specifičnih pitanja. U te podskupine ili na posebne sastanke tih podskupina mogu prema potrebi biti pozvani predstavnici savjetodavnog foruma iz članka 67. kao promatrači.

7. Vijeće za umjetnu inteligenciju organizirano je i djeluje tako da čuva objektivnost i nepristranost svojih aktivnosti.
8. Vijećem za umjetnu inteligenciju predsjedja jedan od predstavnika država članica. Ured za umjetnu inteligenciju osigurava tajništvo Vijeća za umjetnu inteligenciju, saziva sastanke na zahtjev predsjednika i priprema dnevni red u skladu sa zadaćama Vijeća za umjetnu inteligenciju na temelju ove Uredbe i njegovim poslovníkom.

Članak 66.

Zadaci Vijeća za umjetnu inteligenciju

Vijeće za umjetnu inteligenciju savjetuje Komisiju i države članice i pomaže im kako bi se olakšala dosljedna i djelotvorna primjena ove Uredbe. U tom cilju Vijeće za umjetnu inteligenciju posebno može:

- (a) doprinositi koordinaciji među nacionalnim nadležnim tijelima odgovornima za primjenu ove Uredbe i, u suradnji s dotičnim tijelima za nadzor tržišta i podložno njihovoj suglasnosti, podupirati zajedničke aktivnosti tijela za nadzor tržišta iz članka 74. stavka 11.;
- (b) prikupljati i razmjenjivati tehničko i regulatorno stručno znanje i primjere najbolje prakse među državama članicama;
- (c) pružati savjete o provedbi ove Uredbe, posebno u pogledu izvršavanja pravila o UI modelima opće namjene;
- (d) doprinositi usklađivanju administrativnih praksi u državama članicama, među ostalim u pogledu odstupanja od postupaka ocjenjivanja sukladnosti iz članka 46., funkcioniranja regulatornih izoliranih okruženja za umjetnu inteligenciju i testiranja u stvarnim uvjetima iz članaka 57., 59. i 60.;

- (e) na zahtjev Komisije ili na vlastitu inicijativu izdavati preporuke i pisana mišljenja o svim relevantnim pitanjima povezanim s provedbom ove Uredbe i njezinom dosljednom i djelotvornom primjenom, među ostalim:
- i. o izradi i primjeni kodeksâ ponašanja i kodeksâ prakse u skladu s ovom Uredbom, kao i smjernica Komisije;
 - ii. o evaluaciji i preispitivanju ove Uredbe u skladu s člankom 112., među ostalim u pogledu izvješća o ozbiljnim incidentima iz članka 73. i funkcioniranja baze podataka EU-a iz članka 71., o izradi delegiranih akata ili provedbenih akata te u pogledu mogućih usklađivanja ove Uredbe sa zakonodavstvom Unije o usklađivanje navedenim u Prilogu I.;
 - iii. o tehničkim specifikacijama ili postojećim normama u vezi sa zahtjevima utvrđenima u poglavlju III. odjeljku 2.;
 - iv. o upotrebi usklađenih normi ili zajedničkih specifikacija iz članaka 40. i 41.;
 - v. o trendovima, kao što su europska globalna konkurentnost u području umjetne inteligencije, prihvatanje umjetne inteligencije u Uniji i razvoj digitalnih vještina;
 - vi. o trendovima u razvoju tipologije vrijednosnih lanaca umjetne inteligencije, posebno u pogledu posljedica koje iz toga proizlaze u vezi s odgovornošću;

- vii. o mogućoj potrebi za izmjenom Priloga III. u skladu s člankom 7. i o mogućoj potrebi za revizijom članka 5. u skladu s člankom 112., uzimajući u obzir relevantne dostupne dokaze i najnovija tehnološka dostignuća;
- (f) podupirati Komisiju u promicanju pismenosti u području umjetne inteligencije, javne svijesti o koristima, rizicima, zaštitnim mjerama, pravima i obvezama u vezi s korištenjem UI sustava te njihova razumijevanja;
- (g) olakšavati razvoj zajedničkih kriterija i zajedničko razumijevanje relevantnih koncepata predviđenih u ovoj Uredbi među tržišnim operaterima i nadležnim tijelima, među ostalim doprinošenjem razvoju referentnih vrijednosti;
- (h) surađivati, prema potrebi, s drugim institucijama, tijelima, uredima i agencijama Unije te relevantnim Unijanim stručnim skupinama i mrežama, posebno u područjima sigurnosti proizvoda, kibernetičke sigurnosti, tržišnog natjecanja, digitalnih i medijskih usluga, financijskih usluga, zaštite potrošača te zaštite podataka i temeljnih prava;
- (i) doprinositi djelotvornoj suradnji s nadležnim tijelima trećih zemalja i međunarodnim organizacijama;
- (j) pomagati nacionalnim nadležnim tijelima i Komisiji u razvoju organizacijskog i tehničkog stručnog znanja potrebnog za provedbu ove Uredbe, među ostalim doprinošenjem procjeni potreba za osposobljavanjem osoblja država članica uključenog u provedbu ove Uredbe;

- (k) pomagati Uredu za umjetnu inteligenciju u pružanju potpore nacionalnim nadležnim tijelima u uspostavi i razvoju regulatornih izoliranih okruženja za umjetnu inteligenciju te olakšavati suradnju i razmjenu informacija među regulatornim izoliranim okruženjima za umjetnu inteligenciju;
- (l) doprinosti izradi dokumenata sa smjernicama i pružati odgovarajuće savjete o tome;
- (m) savjetovati Komisiju o međunarodnim pitanjima povezanim s umjetnom inteligencijom;
- (n) davati mišljenja Komisiji o kvalificiranim upozorenjima u vezi s UI modelima opće namjene;
- (o) primati mišljenja država članica o kvalificiranim upozorenjima u vezi s UI modelima opće namjene te o nacionalnim iskustvima i nacionalnoj praksi u području praćenja i izvršavanja UI sustava, posebno sustava u koje su integrirani UI modeli opće namjene.

Članak 67.

Savjetodavni forum

1. Osniva se savjetodavni forum koji pruža tehničko stručno znanje i savjetuje Vijeće za umjetnu inteligenciju i Komisiju te doprinosi njihovim zadaćama na temelju ove Uredbe.
2. Članstvo u savjetodavnom forumu čine uravnoteženo odabrani dionici, koji uključuju industriju, *start-up* poduzeća, MSP-ove, civilno društvo i akademsku zajednicu. Članstvo u savjetodavnom forumu mora biti uravnoteženo u smislu komercijalnih i nekomercijalnih interesa, a unutar kategorije komercijalnih interesa uravnoteženo u smislu MSP-ova i ostalih poduzeća.

3. Komisija među dionicima s priznatim stručnim znanjem u području umjetne inteligencije imenuje članove savjetodavnog foruma u skladu s kriterijima iz stavka 2.
4. Mandat članova savjetodavnog foruma traje dvije godine i može se produljiti za najviše četiri godine.
5. Agencija za temeljna prava, ENISA, Europski odbor za normizaciju (CEN), Europski odbor za elektrotehničku normizaciju (CENELEC) i Europski institut za telekomunikacijske norme (ETSI) stalni su članovi savjetodavnog foruma.
6. Savjetodavni forum izrađuje svoj poslovnik. Savjetodavni forum bira dva supredsjednika među svojim članovima, u skladu s kriterijima iz stavka 2. Mandat supredsjednika traje dvije godine i može se jednom produljiti.
7. Savjetodavni forum održava sastanke najmanje dvaput godišnje. Savjetodavni forum na svoje sastanke može pozvati stručnjake i druge dionike.
8. Savjetodavni forum na zahtjev Vijeća za umjetnu inteligenciju ili Komisije može pripremati mišljenja, preporuke i pisane doprinose.
9. Savjetodavni forum može prema potrebi osnovati stalne ili privremene podskupine radi razmatranja posebnih pitanja povezanih s ciljevima ove Uredbe.
10. Savjetodavni forum priprema godišnje izvješće o svojim aktivnostima. To se izvješće objavljuje.

Članak 68.

Znanstveno povjerenstvo neovisnih stručnjaka

1. Komisija provedbenim aktom donosi odredbe o osnivanju znanstvenog povjerenstva neovisnih stručnjaka („znanstveno povjerenstvo”) čija je svrha podupirati aktivnosti izvršavanja na temelju ove Uredbe. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.
2. Znanstveno povjerenstvo sastoji se od stručnjaka koje Komisija odabire na temelju najsuvislijeg znanstvenog ili tehničkog stručnog znanja u području umjetne inteligencije potrebnog za obavljanje zadaća iz stavka 3. i koji moraju moći dokazati da ispunjavaju sve sljedeće uvjete:
 - (a) posjeduju posebno stručno znanje i kompetencije te znanstveno ili tehničko stručno znanje u području umjetne inteligencije;
 - (b) neovisni su od svih dobavljača UI sustava ili UI modela opće namjene;
 - (c) sposobni su aktivnosti provoditi savjesno, točno i objektivno.

Komisija u savjetovanju s Vijećem za umjetnu inteligenciju određuje broj stručnjaka u povjerenstvu u skladu s potrebama i osigurava pravednu rodnu i geografsku zastupljenost.

3. Znanstveno povjerenstvo savjetuje i podupire Ured za umjetnu inteligenciju, posebno u pogledu sljedećih zadaća:
- (a) podupiranja provedbe i izvršavanja ove Uredbe u pogledu UI modela i sustava opće namjene, posebno tako što:
 - i. upozorava Ured za umjetnu inteligenciju o mogućim sistemskim rizicima na razini Unije u pogledu UI modela opće namjene, u skladu s člankom 90.;
 - ii. doprinosi razvoju alata i metodologija za evaluaciju sposobnosti UI modela i sustava opće namjene, među ostalim s pomoću referentnih vrijednosti;
 - iii. pruža savjete o klasifikaciji UI modela opće namjene sa sistemskim rizikom;
 - iv. pruža savjete o klasifikaciji različitih UI modela i sustava opće namjene;
 - v. doprinosi razvoju alata i predložaka;
 - (b) podupiranja rada tijela za nadzor tržišta na njihov zahtjev;
 - (c) podupiranja prekograničnih aktivnosti nadzora tržišta iz članka 74. stavka 11., ne dovodeći u pitanje ovlasti tijela za nadzor tržišta;

(d) podupiranja Ureda za umjetnu inteligenciju u izvršavanju njegovih dužnosti u kontekstu zaštitnog postupka Unije u skladu s člankom 81.

4. Stručnjaci iz znanstvenog povjerenstva svoje zadaće obavljaju nepristrano i objektivno i osiguravaju povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti. Pri obavljanju svojih zadaća iz stavka 3. ne smiju tražiti ni primati upute ni od koga. Svaki stručnjak sastavlja izjavu o interesima, koja se objavljuje. Ured za umjetnu inteligenciju uspostavlja sustave i postupke za aktivno upravljanje mogućim sukobima interesa i njihovo sprečavanje.
5. Provedbeni akt iz stavka 1. uključuje odredbe o uvjetima, postupcima i detaljnim aranžmanima u skladu s kojima znanstveno povjerenstvo i njegovi članovi izdaju upozorenja i traže pomoć Ureda za umjetnu inteligenciju u obavljanju zadaća znanstvenog povjerenstva.

Članak 69.

Pristup država članica stručnjacima

1. Države članice mogu pozvati stručnjake iz znanstvenog povjerenstva da im pruže potporu u njihovim aktivnostima izvršavanja na temelju ove Uredbe.

2. Od država članica može se zahtijevati plaćanje naknada za savjete i potporu stručnjaka. Komisija provedbenim aktom iz članka 68. stavka 1. utvrđuje strukturu i visinu naknada te ljestvicu i strukturu troškova čiji je povrat moguće tražiti, uzimajući u obzir ciljeve adekvatne provedbe ove Uredbe, troškovnu učinkovitost i potrebu da se svim državama članicama osigura djelotvoran pristup stručnjacima.
3. Komisija državama članicama olakšava pravodoban pristup stručnjacima, prema potrebi, i osigurava da kombinacija potpornih aktivnosti koje provode potporna struktura Unije za testiranje umjetne inteligencije u skladu s člankom 84. i stručnjaci u skladu s ovim člankom bude učinkovito organizirana i da donosi najveću moguću dodanu vrijednost.

ODJELJAK 2.

NACIONALNA NADLEŽNA TIJELA

Članak 70.

Imenovanje nacionalnih nadležnih tijela i jedinstvenih kontaktnih točaka

1. Za potrebe ove Uredbe svaka država članica osniva ili imenuje kao nacionalna nadležna tijela barem jedno tijelo koje provodi prijavljivanje i barem jedno tijelo za nadzor tržišta. Ta nacionalna nadležna tijela izvršavaju svoje ovlasti neovisno, nepristrano i bez predrasuda kako bi zaštitila objektivnost svojih aktivnosti i zadaća te osigurala primjenu i provedbu ove Uredbe. Članovi tih tijela suzdržavaju se od svakog djelovanja koje je nespojivo s njihovim dužnostima. Pod uvjetom da se poštuju ta načela, takve aktivnosti i zadaće može obavljati jedno ili više imenovanih tijela, u skladu s organizacijskim potrebama države članice.
2. Države članice obavješćuju Komisiju o identitetu tijela koja provode prijavljivanje i tijela za nadzor tržišta te o zadaćama tih tijela, kao i o svim kasnijim promjenama u vezi s njima. Države članice do ... [12 mjeseci od datuma stupanja na snagu ove Uredbe] elektroničkim komunikacijskim sredstvima objavljuju informacije o tome kako se može stupiti u kontakt s nadležnim tijelima i jedinstvenim kontaktnim točkama. Države članice imenuju tijelo za nadzor tržišta koje će djelovati kao jedinstvena kontaktna točka za ovu Uredbu i obavješćuju Komisiju o identitetu jedinstvene kontaktne točke. Komisija objavljuje popis jedinstvenih kontaktnih točaka.

3. Države članice osiguravaju da njihova nacionalna nadležna tijela imaju adekvatne tehničke, financijske i ljudske resurse i infrastrukturu za djelotvorno obavljanje svojih zadaća na temelju ove Uredbe. Nacionalna nadležna tijela osobito moraju imati dovoljno stalno raspoloživog osoblja čije kompetencije i stručno znanje obuhvaćaju temeljito razumijevanje tehnologija umjetne inteligencije, podataka i obrade podataka, zaštite osobnih podataka, kibernetičke sigurnosti, temeljnih prava i rizika za zdravlje i sigurnost te poznavanje postojećih normi i pravnih zahtjeva. Države članice jednom godišnje ocjenjuju i, ako je to potrebno, ažuriraju zahtjeve u pogledu kompetencija i resursa iz ovog stavka.
4. Nacionalna nadležna tijela poduzimaju odgovarajuće mjere kako bi se osigurala odgovarajuća razina kibernetičke sigurnosti.
5. Pri obavljanju svojih zadaća nacionalna nadležna tijela postupaju u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.
6. Države članice do ... [godinu dana od datuma stupanja na snagu ove Uredbe], a zatim jednom svake dvije godine izvješćuju Komisiju o stanju financijskih i ljudskih resursa nacionalnih nadležnih tijela, uz ocjenu njihove adekvatnosti. Komisija te informacije prosljeđuje Vijeću za umjetnu inteligenciju radi rasprave i utvrđivanja mogućih preporuka.
7. Komisija olakšava razmjenu iskustava među nacionalnim nadležnim tijelima.

8. Nacionalna nadležna tijela mogu pružati smjernice i savjete o provedbi ove Uredbe, posebno MSP-ovima, uključujući *start-up* poduzeća, prema potrebi uzimajući u obzir smjernice i savjete Vijeća za umjetnu inteligenciju i Komisije. Ako nacionalna nadležna tijela namjeravaju pružiti smjernice i savjete u vezi s određenim UI sustavom u područjima obuhvaćenima drugim pravom Unije, prema potrebi se savjetuju s nacionalnim nadležnim tijelima na temelju tog prava Unije.
9. Ako područje primjene ove Uredbe obuhvaća institucije, tijela, urede ili agencije Unije, Europski nadzornik za zaštitu podataka djeluje kao tijelo nadležno za njihov nadzor.

Poglavlje VIII.

Baza podataka EU-a za visokorizične UI sustave

Članak 71.

Baza podataka EU-a za visokorizične UI sustave iz Priloga III.

1. Komisija u suradnji s državama članicama uspostavlja i održava bazu podataka EU-a koja sadržava informacije iz stavaka 2. i 3. ovog članka o visokorizičnim UI sustavima iz članka 6. stavka 2. koji su registrirani u skladu s člancima 49. i 60. i UI sustavima koji se ne smatraju visokorizičnima na temelju članka 6. stavka 3. i koji su registrirani u skladu s člankom 6. stavkom 4. i člankom 49. Pri utvrđivanju funkcionalnih specifikacija te baze podataka Komisija se savjetuje s relevantnim stručnjacima, a pri ažuriranju funkcionalnih specifikacija te baze podataka Komisija se savjetuje s Vijećem za umjetnu inteligenciju.

2. Podatke navedene u odjeljcima A i B Priloga VIII. u bazu podataka EU-a unosi dobavljač ili, ako je primjenjivo, ovlašteni zastupnik.
3. Podatke navedene u odjeljku C Priloga VIII. u bazu podataka EU-a unosi subjekt koji uvodi sustav i koji je tijelo javne vlasti, javna agencija ili javno tijelo ili koji djeluje u ime tijela javne vlasti, javne agencije ili javnog tijela, u skladu s člankom 49. stavcima 3. i 4.
4. Uz iznimku dijela iz članka 49. stavka 4. i članka 60. stavka 4. točke (c), informacije iz baze podataka EU-a registrirane u skladu s člankom 49. moraju biti pristupačne i javno dostupne na način prilagođen korisnicima. Te bi informacije trebale biti jednostavne za snalaženje i strojno čitljive. Informacije registrirane u skladu s člankom 60. dostupne su samo tijelima za nadzor tržišta i Komisiji, osim ako je potencijalni dobavljač ili dobavljač dao privolu da te informacije budu dostupne javnosti.
5. Baza podataka EU-a sadržava osobne podatke samo ako je to potrebno za prikupljanje i obradu informacija u skladu s ovom Uredbom. Te informacije uključuju imena i kontaktne podatke pojedinaca koji su odgovorni za registraciju sustava i koji imaju pravnu ovlast za zastupanje dobavljača ili subjekta koji uvodi sustav, ovisno o slučaju.
6. Komisija je nadzornik baze podataka EU-a. Dobavljačima, potencijalnim dobavljačima i subjektima koji uvode sustav Komisija stavlja na raspolaganje adekvatnu tehničku i administrativnu potporu. Baza podataka EU-a mora ispunjavati primjenjive zahtjeve u pogledu pristupačnosti.

Poglavlje IX.
Praćenje nakon stavljanja na tržište,
razmjena informacija i nadzor tržišta

ODJELJAK 1.
PRAĆENJE NAKON STAVLJANJA NA TRŽIŠTE

Članak 72.

*Praćenje nakon stavljanja na tržište koje provode dobavljači
i plan praćenja nakon stavljanja na tržište za visokorizične UI sustave*

1. Dobavljači uspostavljaju sustav praćenja nakon stavljanja na tržište i izrađuju dokumentaciju za njega na način koji je razmjernan prirodi tehnologija umjetne inteligencije i rizicima visokorizičnog UI sustava.
2. Sustavom praćenja nakon stavljanja na tržište aktivno se i sustavno prikupljaju, dokumentiraju i analiziraju relevantni podaci koje mogu dostaviti subjekti koji uvode sustav ili koji se mogu prikupiti iz drugih izvora o učinkovitosti visokorizičnih UI sustava tijekom cijelog njihova životnog ciklusa i koji dobavljaču omogućuju evaluaciju kontinuirane usklađenosti UI sustava sa zahtjevima iz poglavlja III. odjeljka 2. Ako je to relevantno, praćenje nakon stavljanja na tržište uključuje analizu interakcije s drugim UI sustavima. Ta obveza ne obuhvaća osjetljive operativne podatke subjekata koji uvode sustav koji su tijela kaznenog progona.

3. Sustav praćenja nakon stavljanja na tržište temelji se na planu praćenja nakon stavljanja na tržište. Plan praćenja nakon stavljanja na tržište dio je tehničke dokumentacije iz Priloga IV. Komisija do ... [18 mjeseci od datuma stupanja na snagu ove Uredbe] donosi provedbeni akt s detaljnim odredbama kojima se utvrđuje predložak za plan praćenja nakon stavljanja na tržište i popis elemenata koje treba uključiti u taj plan. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 98. stavka 2.
4. Za visokorizične UI sustave obuhvaćene zakonodavstvom Unije o usklađivanju navedenim u odjeljku A Priloga I., ako su sustav i plan praćenja nakon stavljanja na tržište već uspostavljeni na temelju tog zakonodavstva, kako bi se osigurala dosljednost, izbjeglo udvostručavanje i smanjila dodatna opterećenja, dobavljači imaju mogućnost da, koristeći se predloškom iz stavka 3., potrebne elemente opisane u stavcima 1., 2. i 3. prema potrebi integriraju u sustave i planove koji već postoje na temelju tog zakonodavstva, pod uvjetom da se time postiže jednakovrijedna razina zaštite.

Prvi podstavak ovog stavka primjenjuje se i na visokorizične UI sustave iz točke 5. Priloga III. koje na tržište ili u upotrebu stavljaju financijske institucije na koje se u pogledu njihova unutarnjeg upravljanja, aranžmana ili procesa primjenjuju zahtjevi na temelju prava Unije o financijskim uslugama.

ODJELJAK 2.

RAZMJENA INFORMACIJA O OZBILJNIM INCIDENTIMA

Članak 73.

Prijavljivanje ozbiljnih incidenata

1. Dobavljači visokorizičnih UI sustava stavljenih na tržište Unije prijavljuju svaki ozbiljan incident tijelima za nadzor tržišta država članica u kojima je došlo do tog incidenta.
2. Prijavljivanje iz stavka 1. provodi se odmah nakon što je dobavljač utvrdio uzročno-posljedičnu vezu između UI sustava i ozbiljnog incidenta ili razumnu vjerojatnost takve veze, a u svakom slučaju najkasnije 15 dana nakon što je dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav, saznao za ozbiljni incident.

Razdobljem za prijavljivanje iz prvog podstavka uzima se u obzir težina ozbiljnog incidenta.

3. Neovisno o stavku 2. ovog članka, u slučaju raširene povrede ili ozbiljnog incidenta kako je definiran u članku 3. točki 49. podtočki (b), prijavljivanje iz stavka 1. ovog članka provodi se odmah, a najkasnije dva dana nakon što dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav, sazna za taj incident.

4. Neovisno o stavku 2., u slučaju smrti osobe prijavljivanje se provodi odmah nakon što je dobavljač ili subjekt koji uvodi sustav utvrdio uzročno-posljedičnu vezu između visokorizičnog UI sustava i ozbiljnog incidenta ili čim je posumnjao u postojanje takve veze, a najkasnije deset dana nakon datuma na koji je dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav, saznao za ozbiljni incident.
5. Ako je to potrebno kako bi se osiguralo pravodobno prijavljivanje, dobavljač ili, ako je primjenjivo, subjekt koji uvodi sustav može podnijeti početnu prijavu koja je nepotpuna, nakon koje slijedi potpuna prijava.
6. Nakon prijavljivanja ozbiljnog incidenta u skladu sa stavkom 1. dobavljač bez odgode provodi potrebne istrage u vezi s ozbiljnim incidentom i dotičnim UI sustavom. To uključuje procjenu rizika incidenta i korektivne mjere.

Dobavljač surađuje s nadležnim tijelima i, prema potrebi, s dotičnim prijavljenim tijelom tijekom istraga iz prvog podstavka i ne provodi istragu koja uključuje izmjenu dotičnog UI sustava na način koji bi mogao utjecati na naknadnu evaluaciju uzroka incidenta prije nego što o takvom djelovanju obavijesti nadležna tijela.
7. Nakon primitka obavijesti o ozbiljnom incidentu iz članka 3. točke 49. podtočke (c) relevantno tijelo za nadzor tržišta o tome obavješćuje nacionalna tijela javne vlasti ili javna tijela iz članka 77. stavka 1. Komisija izrađuje namjenske smjernice za lakše ispunjavanje obveza utvrđenih u stavku 1. ovog članka. Te se smjernice izdaju do ... [12 mjeseci od stupanja na snagu ove Uredbe] i redovito se ocjenjuju.

8. Tijelo za nadzor tržišta u roku od sedam dana od datuma na koji je primilo prijavu iz stavka 1. ovog članka poduzima odgovarajuće mjere, kako je predviđeno u članku 19. Uredbe (EU) 2019/1020, i slijedi postupke prijavljivanja predviđene u toj uredbi.
9. Za visokorizične UI sustave iz Priloga III. koje na tržište ili u upotrebu stavljaju dobavljači na koje se primjenjuju zakonodavni instrumenti Unije kojima se utvrđuju obveze izvješćivanja jednakovrijedne onima koje su utvrđene u ovoj Uredbi, prijavljivanje ozbiljnih incidenata ograničava se na ozbiljne incidente iz članka 3. točke 49. podtočke (c).
10. Za visokorizične UI sustave koji su sigurnosne komponente uređaja ili su sami uređaji, a obuhvaćeni su uredbama (EU) 2017/745 i (EU) 2017/746, prijava ozbiljnih incidenata ograničava se na ozbiljne incidente iz članka 3. točke 49. podtočke (c) ove Uredbe i upućuje se nacionalnom nadležnom tijelu koje su u tu svrhu odabrale države članice u kojima je došlo do incidenta.
11. Nacionalna nadležna tijela odmah prijavljuju Komisiji svaki ozbiljan incident u skladu s člankom 20. Uredbe (EU) 2019/1020, bez obzira na to jesu li u vezi s njim poduzela mjere.

ODJELJAK 3.

IZVRŠAVANJE

Članak 74.

Nadzor nad tržištem i kontrola UI sustava na tržištu Unije

1. Uredba (EU) 2019/1020 primjenjuje se na UI sustave obuhvaćene ovom Uredbom.
U svrhu djelotvornog izvršavanja ove Uredbe:
 - (a) smatra se da svako upućivanje na gospodarski subjekt na temelju Uredbe (EU) 2019/1020 uključuje sve operatere iz članka 2. stavka 1. ove Uredbe;
 - (b) smatra se da svako upućivanje na proizvod na temelju Uredbe (EU) 2019/1020 uključuje sve UI sustave obuhvaćene područjem primjene ove Uredbe.
2. U okviru svojih obveza izvješćivanja na temelju članka 34. stavka 4. Uredbe (EU) 2019/1020 tijela za nadzor tržišta svake godine izvješćuju Komisiju i relevantna nacionalna tijela nadležna za tržišno natjecanje o svim informacijama utvrđenima tijekom aktivnosti nadzora tržišta koje bi mogle biti od interesa za primjenu prava Unije o pravilima tržišnog natjecanja. Također svake godine izvješćuju Komisiju o primjeni zabranjenih praksi do koje je došlo tijekom te godine i o poduzetim mjerama.
3. Za visokorizične UI sustave povezane s proizvodima na koje se primjenjuje zakonodavstvo Unije o usklađivanju navedeno u odjeljku A Priloga I. tijelo za nadzor tržišta za potrebe ove Uredbe tijelo je odgovorno za aktivnosti nadzora tržišta imenovano na temelju tih pravnih akata.

Odstupajući od prvog podstavka i u primjerenim okolnostima, države članice mogu imenovati drugo relevantno tijelo koje će djelovati kao tijelo za nadzor tržišta pod uvjetom da osiguraju koordinaciju s relevantnim sektorskim tijelima za nadzor tržišta odgovornima za izvršavanje zakonodavstva Unije o usklađivanju navedenog u Prilogu I.

4. Postupci iz članaka od 79. do 83. ove Uredbe ne primjenjuju se na UI sustave povezane s proizvodima na koje se primjenjuje zakonodavstvo Unije o usklađivanju navedeno u odjeljku A Priloga I. ako su tim pravnim aktima već predviđeni postupci kojima se osigurava jednakovrijedna razina zaštite i ako ti pravni akti imaju isti cilj. U takvim se slučajevima primjenjuju relevantni sektorski postupci.
5. Ne dovodeći u pitanje ovlasti tijela za nadzor tržišta na temelju članka 14. Uredbe (EU) 2019/1020, u svrhu osiguravanja djelotvornog izvršavanja ove Uredbe tijela za nadzor tržišta ovlasti iz članka 14. stavka 4. točaka (d) i (j) te uredbe mogu, prema potrebi, izvršavati na daljinu.
6. Za visokorizične UI sustave koji se stavljaju na tržište, stavljaju u upotrebu ili koje koriste financijske institucije regulirane pravom Unije o financijskim uslugama, tijelo za nadzor tržišta za potrebe ove Uredbe relevantno je nacionalno tijelo odgovorno za financijski nadzor tih institucija na temelju tog zakonodavstva ako su stavljanje na tržište, stavljanje u upotrebu ili korištenje UI sustava izravno povezani s pružanjem tih financijskih usluga.

7. Odstupajući od stavka 6., u primjerenim okolnostima i pod uvjetom da je osigurana koordinacija, država članica može odrediti drugo relevantno tijelo kao tijelo za nadzor tržišta za potrebe ove Uredbe.

Nacionalna tijela za nadzor tržišta koja nadziru regulirane kreditne institucije regulirane Direktivom 2013/36/EU, a koje sudjeluju u jedinstvenom nadzornom mehanizmu uspostavljenom Uredbom (EU) br. 1024/2013, trebala bi bez odgode izvijestiti Europsku središnju banku o svim informacijama utvrđenima tijekom njihovih aktivnosti nadzora tržišta koje bi mogle biti od interesa za zadaće bonitetnog nadzora Europske središnje banke navedene u toj uredbi.

8. Za visokorizične UI sustave iz točke 1. Priloga III. ovoj Uredbi, ako se ti sustavi upotrebljavaju u svrhu kaznenog progona, upravljanja granicama, pravosuđa i demokracije, te za visokorizične UI sustave navedene u točkama 6., 7. i 8. Priloga III. ovoj Uredbi, države članice za potrebe ove Uredbe kao tijela za nadzor tržišta imenuju ili nadležna nadzorna tijela za zaštitu podataka na temelju Uredbe (EU) 2016/679 ili Direktive (EU) 2016/680 ili bilo koje drugo tijelo imenovano u skladu s istim uvjetima, utvrđenima u člancima od 41. do 44. Direktive (EU) 2016/680. Aktivnosti nadzora tržišta ni na koji način ne smiju utjecati na neovisnost pravosudnih tijela niti smiju na drugi način utjecati na njihove aktivnosti kada djeluju u pravosudnom svojstvu.

9. Ako područje primjene ove Uredbe obuhvaća institucije, tijela, urede ili agencije Unije, Europski nadzornik za zaštitu podataka djeluje kao njihovo tijelo za nadzor tržišta, osim u odnosu na Sud Europske unije kada djeluje u svojem sudbenom svojstvu.
10. Države članice olakšavaju koordinaciju između tijela za nadzor tržišta imenovanih na temelju ove Uredbe i drugih relevantnih nacionalnih tijela koja nadziru primjenu prava Unije o usklađivanju navedenog u Prilogu I. ili drugog prava Unije koje bi moglo biti relevantno za visokorizične UI sustave iz Priloga III.
11. Tijela za nadzor tržišta i Komisija mogu predložiti zajedničke aktivnosti, uključujući zajedničke istrage, koje trebaju provesti tijela za nadzor tržišta ili tijela za nadzor tržišta zajedno s Komisijom, a čiji je cilj promicanje usklađenosti, utvrđivanje neusklađenosti, podizanje svijesti ili pružanje smjernica u vezi s ovom Uredbom u pogledu specifičnih kategorija visokorizičnih UI sustava za koje je utvrđeno da predstavljaju ozbiljan rizik u dvjema ili više država članica u skladu s člankom 9. Uredbe (EU) 2019/1020. Ured za umjetnu inteligenciju pruža koordinacijsku potporu za zajedničke istrage.

12. Ne dovodeći u pitanje ovlasti predviđene na temelju Uredbe (EU) 2019/1020 te, ako je to relevantno i ograničeno na ono što je potrebno za ispunjavanje njihovih zadaća, dobavljači tijelima za nadzor tržišta odobravaju puni pristup dokumentaciji i skupovima podataka za treniranje, validaciju i testiranje koji se upotrebljavaju za razvoj visokorizičnih UI sustava, među ostalim, prema potrebi i podložno sigurnosnim zaštitnim mjerama, putem aplikacijskih programskih sučelja ili drugih relevantnih tehničkih sredstava i alata koji omogućuju daljinski pristup.
13. Tijelima za nadzor tržišta odobrava se pristup izvornom kodu visokorizičnog UI sustava na obrazložen zahtjev i samo ako su ispunjena sljedeća dva uvjeta:
- (a) pristup izvornom kodu potreban je za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2.; i
 - (b) postupci testiranja ili revizije i provjere na temelju podataka i dokumentacije koje je dostavio dobavljač iscrpljeni su ili su se pokazali nedostatnima.
14. Sa svim informacijama ili dokumentacijom koje su tijela za nadzor tržišta dobila postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 75.

Uzajamna pomoć, nadzor tržišta i kontrola UI sustavâ opće namjene

1. Ako se UI sustav temelji na UI modelu opće namjene, a model i sustav razvija isti dobavljač, Ured za umjetnu inteligenciju ima ovlasti za praćenje i nadzor usklađenosti tog UI sustava s obvezama na temelju ove Uredbe. Za obavljanje svojih zadaća praćenja i nadzora Ured za umjetnu inteligenciju ima sve ovlasti tijela za nadzor tržišta predviđene u ovom odjeljku i u Uredbi (EU) 2019/1020.
2. Ako relevantna tijela za nadzor tržišta imaju dovoljno razloga smatrati da UI sustavi opće namjene koje subjekti koji uvode sustav mogu izravno upotrebljavati u barem jednu svrhu koja je na temelju ove Uredbe klasificirana kao visokorizična nisu usklađeni sa zahtjevima ove Uredbe, ona surađuju s Uredom za umjetnu inteligenciju kako bi provela evaluacije usklađenosti i o tome obavješćuju Vijeće za umjetnu inteligenciju i druga tijela za nadzor tržišta.

3. Ako tijelo za nadzor tržišta ne može zaključiti svoju istragu visokorizičnog UI sustava zbog toga što nema pristup određenim informacijama povezanim s UI modelom opće namjene, iako je poduzelo sve potrebne korake kako bi ih pribavilo, ono može Uredu za umjetnu inteligenciju podnijeti obrazloženi zahtjev na temelju kojeg se nalaže pristup tim informacijama. U tom slučaju Ured za umjetnu inteligenciju bez odgode, a najkasnije u roku od 30 dana, tijelu podnositelju zahtjeva dostavlja sve informacije koje Ured za umjetnu inteligenciju smatra važnima za utvrđivanje je li visokorizični UI sustav neusklađen. Tijela za nadzor tržišta štite povjerljivost informacija koje su pribavila u skladu s člankom 78. ove Uredbe. Postupak predviđen u poglavlju VI. Uredbe (EU) 2019/1020 primjenjuje se *mutatis mutandis*.

Članak 76.

Nadzor testiranja u stvarnim uvjetima koji provode tijela za nadzor tržišta

1. Tijela za nadzor tržišta imaju nadležnosti i ovlasti da osiguraju da se testiranje u stvarnim uvjetima provodi u skladu s ovom Uredbom.
2. Ako se testiranje u stvarnim uvjetima provodi za UI sustave koji se nadziru u regulatornom izoliranom okruženju za umjetnu inteligenciju na temelju članka 58., tijela za nadzor tržišta provjeravaju usklađenost s člankom 60. u okviru svoje nadzorne uloge za regulatorno izolirano okruženje za umjetnu inteligenciju. Ta tijela mogu, prema potrebi, dopustiti da dobavljač ili potencijalni dobavljač provodi testiranje u stvarnim uvjetima odstupajući od uvjeta utvrđenih u članku 60. stavku 4. točaka (f) i (g).

3. Ako su potencijalni dobavljač, dobavljač ili treća strana obavijestili tijelo za nadzor tržišta o ozbiljnom incidentu ili ono ima drugih razloga vjerovati da uvjeti iz članaka 60. i 61. nisu ispunjeni, ono može na svojem državnom području prema potrebi donijeti jednu od sljedećih odluka:
- (a) suspendirati ili obustaviti testiranje u stvarnim uvjetima;
 - (b) zahtijevati od dobavljača ili potencijalnog dobavljača i od subjekta koji uvodi sustav ili potencijalnog subjekta koji uvodi sustav da izmijeni bilo koji aspekt testiranja u stvarnim uvjetima.
4. Ako je tijelo za nadzor tržišta donijelo odluku iz stavka 3. ovog članka ili je podnijelo prigovor u smislu članka 60. stavka 4. točke (b), u odluci ili prigovoru moraju se navesti razlozi za njih te način na koji dobavljač ili potencijalni dobavljač može osporiti odluku ili prigovor.
5. Kada je primjenjivo, ako je tijelo za nadzor tržišta donijelo odluku iz stavka 3., o razlozima njezina donošenja obavješćuje tijela za nadzor tržišta drugih država članica u kojima je UI sustav testiran u skladu s planom testiranja.

Članak 77.

Ovlasti tijela nadležnih za zaštitu temeljnih prava

1. Nacionalna tijela javne vlasti ili javna tijela koja nadziru ili izvršavaju poštovanje obveza na temelju prava Unije o zaštiti temeljnih prava, uključujući pravo na nediskriminaciju, u pogledu korištenja visokorizičnih UI sustava iz Priloga III. ovlaštena su zatražiti i pristupiti svojoj dokumentaciji izrađenoj ili vođenoj na temelju ove Uredbe na pristupačnom jeziku i u pristupačnom formatu kada je pristup toj dokumentaciji potreban za djelotvorno ispunjavanje njihovih mandata u granicama njihove jurisdikcije. Relevantno tijelo javne vlasti ili javno tijelo obavješćuje tijelo za nadzor tržišta dotične države članice o svakom takvom zahtjevu.
2. Svaka država članica do ... [tri mjeseca od stupanja na snagu ove Uredbe] određuje tijela javne vlasti ili javna tijela iz stavka 1. i objavljuje popis tih tijela. Države članice taj popis dostavljaju Komisiji i drugim državama članicama te ga ažuriraju.
3. Ako dokumentacija iz stavka 1. nije dovoljna za utvrđivanje je li došlo do povrede obveza na temelju prava Unije o zaštiti temeljnih prava, tijelo javne vlasti ili javno tijelo iz stavka 1. može tijelu za nadzor tržišta podnijeti obrazloženi zahtjev za organiziranje testiranja visokorizičnog UI sustava tehničkim sredstvima. Tijelo za nadzor tržišta u razumnom roku nakon podnošenja zahtjeva organizira testiranje u bliskoj suradnji s tijelom javne vlasti ili javnim tijelom koje je podnijelo zahtjev.

4. Sa svim informacijama ili dokumentacijom koje su nacionalna tijela javne vlasti ili javna tijela iz stavka 1. ovog članka dobila na temelju ovog članka postupa se u skladu s obvezama u pogledu povjerljivosti utvrđenima u članku 78.

Članak 78.

Povjerljivost

1. Komisija, tijela za nadzor tržišta, prijavljena tijela i sve druge fizičke ili pravne osobe uključene u primjenu ove Uredbe, u skladu s pravom Unije ili nacionalnim pravom, poštuju povjerljivost informacija i podataka dobivenih pri obavljanju svojih zadaća i aktivnosti tako da osobito štite:
- (a) prava intelektualnog vlasništva i povjerljive poslovne informacije ili poslovne tajne fizičke ili pravne osobe, uključujući izvorni kôd, osim u slučajevima iz članka 5. Direktive (EU) 2016/943 Europskog parlamenta i Vijeća⁵⁷;
 - (b) djelotvornu provedbu ove Uredbe, osobito za potrebe inspekcija, istraga ili revizija;
 - (c) javne i nacionalne sigurnosne interese;
 - (d) provedbu kaznenih ili upravnih postupaka;

⁵⁷ Direktiva (EU) 2016/943 Europskog parlamenta i Vijeća od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja (SL L 157, 15.6.2016., str. 1.).

(e) podatke klasificirane na temelju prava Unije ili nacionalnog prava.

2. Tijela uključena u primjenu ove Uredbe u skladu sa stavkom 1. zahtijevaju samo one podatke koji su nužni za procjenu rizika koji predstavljaju UI sustavi i za izvršavanje svojih ovlasti u skladu s ovom Uredbom i s Uredbom (EU) 2019/1020. Ta tijela uspostavljaju adekvatne i djelotvorne mjere u području kibernetičke sigurnosti radi zaštite sigurnosti i povjerljivosti dobivenih informacija i podataka te u skladu s primjenjivim pravom Unije ili nacionalnim pravom brišu prikupljene podatke čim prestanu biti potrebni u svrhu za koju su dobiveni.
3. Ne dovodeći u pitanje stavke 1. i 2., informacije koje na povjerljivoj osnovi međusobno razmjenjuju nacionalna nadležna tijela ili nacionalna nadležna tijela i Komisija ne otkrivaju se bez prethodnog savjetovanja s nacionalnim nadležnim tijelom od kojeg informacije potječu i sa subjektom koji uvodi sustav kada tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil upotrebljavaju visokorizične UI sustave iz točaka 1., 6. ili 7. Priloga III. i kada bi se takvim otkrivanjem ugrozili javni i nacionalni sigurnosni interesi. Ta razmjena informacija ne obuhvaća osjetljive operativne podatke u vezi s aktivnostima tijela kaznenog progona, tijela za nadzor granica, tijela za imigraciju ili tijela za azil.

Ako su tijela kaznenog progona, tijela za imigraciju ili tijela za azil dobavljači visokorizičnih UI sustava iz točaka 1., 6. ili 7. Priloga III., tehnička dokumentacija iz Priloga IV. ostaje u prostorijama tih tijela. Ta tijela osiguravaju da tijela za nadzor tržišta iz članka 74. stavaka 8. i 9., ovisno o slučaju, mogu na zahtjev odmah pristupiti toj dokumentaciji ili dobiti njezin primjerak. Pristup toj dokumentaciji ili njezinim primjercima dopušten je samo osoblju tijela za nadzor tržišta koje je prošlo odgovarajući stupanj sigurnosne provjere.

4. Stavci 1., 2. i 3. ne utječu na prava ili obveze Komisije, država članica i njihovih relevantnih tijela, kao ni na obveze prijavljenih tijela u pogledu razmjene informacija i širenja upozorenja, među ostalim u kontekstu prekogranične suradnje, a ne utječu ni na obveze dotičnih stranaka da pruže informacije na temelju kaznenog prava država članica.
5. Komisija i države članice mogu, kada je to potrebno i u skladu s relevantnim odredbama međunarodnih i trgovinskih sporazuma, razmjenjivati povjerljive informacije s regulatornim tijelima trećih zemalja s kojima su sklopile bilateralne ili multilateralne aranžmane o povjerljivosti kojima se jamči odgovarajuća razina povjerljivosti.

Članak 79.

Postupak koji se na nacionalnoj razini primjenjuje na UI sustave koji predstavljaju rizik

1. UI sustavi koji predstavljaju rizik smatraju se „proizvodom koji predstavlja rizik” kako je definiran u članku 3. točki 19. Uredbe (EU) 2019/1020 u mjeri u kojoj predstavljaju rizike za zdravlje ili sigurnost osoba ili za temeljna prava osoba.

2. Ako tijelo za nadzor tržišta države članice ima dovoljno razloga smatrati da UI sustav predstavlja rizik u smislu stavka 1. ovog članka, ono evaluira usklađenost dotičnog UI sustava sa svim zahtjevima i obvezama utvrđenima u ovoj Uredbi. Posebna pozornost posvećuje se UI sustavima koji predstavljaju rizik za skupine ranjivih osoba. Ako su utvrđeni rizici za temeljna prava, tijelo za nadzor tržišta ujedno obavješćuje relevantna nacionalna tijela javne vlasti ili javna tijela iz članka 77. stavka 1. te s njima u potpunosti surađuje. Relevantni operateri prema potrebi surađuju s tijelom za nadzor tržišta i drugim nacionalnim tijelima javne vlasti ili javnim tijelima iz članka 77. stavka 1.

Ako tijekom te evaluacije tijelo za nadzor tržišta ili, ako je primjenjivo, tijelo za nadzor tržišta u suradnji s nacionalnim tijelom javne vlasti iz članka 77. stavka 1. utvrdi da UI sustav ne ispunjava zahtjeve i obveze utvrđene u ovoj Uredbi, ono bez nepotrebne odgode od relevantnog operatera zahtijeva da poduzme sve odgovarajuće korektivne mjere kako bi UI sustav uskladio s tim zahtjevima i obvezama, povukao ga s tržišta ili ga opozvao u roku koji može propisati tijelo za nadzor tržišta, a u svakom slučaju unutar manje od 15 radnih dana ili kako je predviđeno u relevantnom zakonodavstvu Unije o usklađivanju.

Tijelo za nadzor tržišta o tome obavješćuje relevantno prijavljeno tijelo. Na mjere navedene u drugom podstavku ovog stavka primjenjuje se članak 18. Uredbe (EU) 2019/1020.

3. Ako tijelo za nadzor tržišta smatra da neusklađenost nije ograničena samo na njegovo državno područje, ono bez nepotrebne odgode obavješćuje Komisiju i druge države članice o rezultatima evaluacije i mjerama za koje je zatražilo da ih operater poduzme.
4. Operater osigurava da se poduzmu sve odgovarajuće korektivne mjere u pogledu svih dotičnih UI sustava koje je stavio na raspolaganje na tržištu Unije.
5. Ako operater UI sustava ne poduzme adekvatne korektivne mjere u roku iz stavka 2., tijelo za nadzor tržišta poduzima sve odgovarajuće privremene mjere kako bi zabranilo ili ograničilo stavljanje UI sustava na raspolaganje na svojem nacionalnom tržištu ili njegovo stavljanje u upotrebu, odnosno kako bi povuklo taj proizvod ili samostalan UI sustav s tog tržišta ili ga opozvalo. To tijelo bez nepotrebne odgode obavješćuje Komisiju i druge države članice o navedenim mjerama.
6. Obavijest iz stavka 5. uključuje sve dostupne pojedinosti, a osobito informacije potrebne za identifikaciju neusklađenog UI sustava, njegovo podrijetlo i lanac opskrbe, prirodu navodne neusklađenosti i povezanog rizika, prirodu i trajanje poduzetih nacionalnih mjera te argumente relevantnog operatera. Tijela za nadzor tržišta posebno navode je li neusklađenost posljedica jednog ili više sljedećih uzroka:
 - (a) ne poštuje se zabrana praksi u području umjetne inteligencije iz članka 5.;
 - (b) visokorizični UI sustav ne ispunjava zahtjeve utvrđene u poglavlju III. odjeljku 2.;

- (c) postoje nedostaci u usklađenim normama ili zajedničkim specifikacijama iz članaka 40. i 41. kojima se stvara pretpostavka sukladnosti;
 - (d) izostaje usklađenost s člankom 50.
7. Tijela za nadzor tržišta koja nisu tijelo za nadzor tržišta države članice koje pokreće postupak bez nepotrebne odgode obavješćuju Komisiju i druge države članice o svim donesenim mjerama i o svim dodatnim informacijama koje su im na raspolaganju i koje se odnose na neusklađenost dotičnog UI sustava te, u slučaju neslaganja s nacionalnom mjerom o kojoj je obaviješteno, o svojim prigovorima.
8. Ako u roku od tri mjeseca od primitka obavijesti iz stavka 5. ovog članka ni tijelo za nadzor tržišta države članice ni Komisija ne podnese prigovor na privremenu mjeru koju je poduzelo tijelo za nadzor tržišta druge države članice, ta mjera smatra se opravdanom. Time se ne dovode u pitanje postupovna prava dotičnog operatera u skladu s člankom 18. Uredbe (EU) 2019/1020. Tromjesečno razdoblje iz ovog stavka skraćuje se na 30 dana u slučaju nepoštovanja zabrane praksi u području umjetne inteligencije iz članka 5. ove Uredbe.
9. Tijela za nadzor tržišta osiguravaju da se u odnosu na dotični proizvod ili UI sustav bez nepotrebne odgode poduzmu primjerene restriktivne mjere, primjerice povlačenje proizvoda ili UI sustava s njihovih tržišta.

Članak 80.

*Postupak koji se primjenjuje na UI sustave koje je dobavljač
u skladu s Prilogom III. klasificirao kao UI sustave koji nisu visokorizični*

1. Ako tijelo za nadzor tržišta ima dovoljno razloga smatrati da UI sustav koji je dobavljač u skladu s člankom 6. stavkom 3. klasificirao kao UI sustav koji nije visokorizičan zapravo jest visokorizičan, ono provodi evaluaciju dotičnog UI sustava u vezi s njegovom klasifikacijom kao visokorizičnim UI sustavom na temelju uvjeta utvrđenih u članku 6. stavku 3. i smjernica Komisije.
2. Ako tijekom te evaluacije tijelo za nadzor tržišta utvrdi da je dotični UI sustav visokorizičan, ono od relevantnog dobavljača bez nepotrebne odgode zahtijeva da poduzme sve potrebne mjere kako bi UI sustav uskladio sa zahtjevima i obvezama utvrđenima u ovoj Uredbi te da u roku koji može propisati tijelo za nadzor tržišta poduzme odgovarajuće korektivne mjere.
3. Ako tijelo za nadzor tržišta smatra da korištenje dotičnog UI sustava nije ograničeno samo na njegovo državno područje, ono bez nepotrebne odgode Komisiju i druge države članice obavješćuje o rezultatima evaluacije i mjerama za koje je zatražilo da ih dobavljač poduzme.

4. Dobavljač osigurava da se poduzmu sve potrebne mjere kako bi se UI sustav uskladio sa zahtjevima i obvezama utvrđenima u ovoj Uredbi. Ako dobavljač dotičnog UI sustava u roku iz stavka 2. ovog članka ne uskladi taj UI sustav s navedenim zahtjevima i obvezama, izriču mu se novčane kazne u skladu s člankom 99.
5. Dobavljač osigurava da se poduzmu sve odgovarajuće korektivne mjere u pogledu svih dotičnih UI sustava koje je stavio na raspolaganje na tržištu Unije.
6. Ako dobavljač dotičnog UI sustava u roku iz stavka 2. ovog članka ne poduzme odgovarajuće korektivne mjere, primjenjuje se članak 79. stavci od 5. do 9.
7. Ako tijekom evaluacije na temelju stavka 1. ovog članka tijelo za nadzor tržišta utvrdi da je dobavljač pogrešno klasificirao UI sustav kao UI sustav koji nije visokorizičan kako bi izbjegao primjenu zahtjeva iz poglavlja III. odjeljka 2., dobavljaču se izriču novčane kazne u skladu s člankom 99.
8. Pri izvršavanju svojih ovlasti za praćenje primjene ovog članka, a u skladu s člankom 11. Uredbe (EU) 2019/1020, tijela za nadzor tržišta mogu provoditi odgovarajuće provjere, posebno uzimajući u obzir informacije pohranjene u bazi podataka EU-a iz članka 71. ove Uredbe.

Članak 81.

Zaštitni postupak Unije

1. Ako tijelo za nadzor tržišta države članice u roku od tri mjeseca od primitka obavijesti iz članka 79. stavka 5., ili u roku od 30 dana u slučaju nepoštovanja zabrane praksi u području umjetne inteligencije iz članka 5., podnese prigovore na mjeru koju je poduzelo drugo tijelo za nadzor tržišta ili ako Komisija smatra da je mjera u suprotnosti s pravom Unije, Komisija bez nepotrebne odgode započinje savjetovanje s tijelom za nadzor tržišta relevantne države članice i operaterom ili operaterima te provodi evaluaciju nacionalne mjere. Na temelju rezultata te evaluacije Komisija u roku od šest mjeseci, ili u roku od 60 dana u slučaju nepoštovanja zabrane praksi u području umjetne inteligencije iz članka 5., od obavijesti iz članka 79. stavka 5. odlučuje je li nacionalna mjera opravdana i svoju odluku priopćuje tijelu za nadzor tržišta dotične države članice. Komisija o svojoj odluci obavještuje i sva ostala tijela za nadzor tržišta.
2. Ako Komisija smatra da je mjera koju je poduzela relevantna država članica opravdana, sve države članice osiguravaju da u vezi s dotičnim UI sustavom poduzmu primjerene restriktivne mjere, primjerice tako da zahtijevaju da se taj UI sustav bez nepotrebne odgode povuče s njihova tržišta, i o tome obavještuju Komisiju. Ako Komisija smatra da je nacionalna mjera neopravdana, dotična država članica povlači mjeru i o tome obavještuje Komisiju.

3. Ako se nacionalna mjera smatra opravdanom i ako se neusklađenost UI sustava pripisuje nedostacima u usklađenim normama ili zajedničkim specifikacijama iz članaka 40. i 41. ove Uredbe, Komisija primjenjuje postupak iz članka 11. Uredbe (EU) br. 1025/2012.

Članak 82.

Usklađeni UI sustavi koji predstavljaju rizik

1. Ako tijelo za nadzor tržišta države članice nakon provedene evaluacije na temelju članka 79. i savjetovanja s relevantnim nacionalnim tijelom javne vlasti iz članka 77. stavka 1. zaključi da visokorizični UI sustav, iako je u skladu s ovom Uredbom, ipak predstavlja rizik za zdravlje ili sigurnost osoba, za temeljna prava ili za druge aspekte zaštite javnog interesa, od relevantnog operatera zahtijeva da bez nepotrebne odgode i u roku koji ono može propisati poduzme sve odgovarajuće mjere kako bi se osiguralo da dotični UI sustav, kada bude stavljen na tržište ili u upotrebu, više ne predstavlja taj rizik.
2. Dobavljač ili drugi relevantni operater osigurava da se u roku koji je propisalo tijelo za nadzor tržišta države članice iz stavka 1. poduzmu korektivne mjere u pogledu dotičnih UI sustava koje je stavio na raspolaganje na tržištu Unije.

3. Države članice odmah obavješćuju Komisiju i druge države članice o zaključku na temelju stavka 1. Te informacije uključuju sve dostupne pojedinosti, a osobito podatke potrebne za identifikaciju dotičnog UI sustava, podrijetlo i lanac opskrbe tog UI sustava, prirodu s njime povezanog rizika te prirodu i trajanje poduzetih nacionalnih mjera.
4. Komisija bez nepotrebne odgode započinje savjetovanje s dotičnim državama članicama i relevantnim operaterima te provodi evaluaciju poduzetih nacionalnih mjera. Na temelju rezultata te evaluacije Komisija odlučuje je li mjera opravdana i prema potrebi predlaže druge odgovarajuće mjere.
5. Komisija svoju odluku odmah priopćuje dotičnim državama članicama i relevantnim operaterima. Komisija o njoj obavješćuje i druge države članice.

Članak 83.

Formalna neusklađenost

1. Tijelo za nadzor tržišta države članice od relevantnog dobavljača zahtijeva da određenu neusklađenost otkloni u roku koji ono može propisati ako ustanovi jedno od sljedećeg:
 - (a) oznaka CE stavljena je uz kršenje članka 48.;
 - (b) oznaka CE uopće nije stavljena;
 - (c) EU izjava o sukladnosti iz članka 47. nije sastavljena;

- (d) EU izjava o sukladnosti iz članka 47. nije ispravno sastavljena;
 - (e) registracija u bazi podataka EU-a iz članka 71. nije provedena;
 - (f) ovlašteni zastupnik nije imenovan, ako je primjenjivo;
 - (g) tehnička dokumentacija nije dostupna.
2. Ako se neusklađenost iz stavka 1. nastavi, tijelo za nadzor tržišta dotične države članice poduzima odgovarajuće i razmjerne mjere kako bi ograničilo ili zabranilo stavljanje visokorizičnog UI sustava na raspolaganje na tržištu ili kako bi osiguralo da se taj UI sustav bez odgode opozove ili povuče s tržišta.

Članak 84.

Potporne strukture Unije za testiranje umjetne inteligencije

1. Komisija za obavljanje zadaća na temelju članka 21. stavka 6. Uredbe (EU) 2019/1020 u području umjetne inteligencije određuje jednu ili više potpornih struktura Unije za testiranje umjetne inteligencije.
2. Ne dovodeći u pitanje zadaće iz stavka 1., potporne strukture Unije za testiranje umjetne inteligencije također pružaju neovisne tehničke ili znanstvene savjete na zahtjev Vijeća za umjetnu inteligenciju, Komisije ili tijelâ za nadzor tržišta.

ODJELJAK 4.

PRAVNA SREDSTVA

Članak 85.

Pravo na podnošenje pritužbe tijelu za nadzor tržišta

Ne dovodeći u pitanje druga upravna ili sudska pravna sredstva, svaka fizička ili pravna osoba koja ima razloga smatrati da je došlo do povrede odredaba ove Uredbe može podnijeti pritužbe relevantnom tijelu za nadzor tržišta.

U skladu s Uredbom (EU) 2019/1020 takve pritužbe uzimaju se u obzir u svrhu provođenja aktivnosti nadzora tržišta i s njima se postupa u skladu s posebnim postupcima koje su u tu svrhu utvrdila tijela za nadzor tržišta.

Članak 86.

Pravo na objašnjenje donošenja pojedinačnih odluka

1. Svaka osoba na koju se primjenjuje odluka koju subjekt koji uvodi sustav donese na temelju izlaznih podataka visokorizičnog UI sustava iz Priloga III., uz iznimku sustava navedenih u točki 2. tog priloga, a koja proizvodi pravne učinke ili na tu osobu na sličan način znatno utječe tako da ona smatra da ima negativan učinak na njezino zdravlje, sigurnost ili temeljna prava, ima pravo od subjekta koji uvodi sustav zatražiti jasna i smislena objašnjenja o ulozi UI sustava u postupku donošenja odluka i o glavnim elementima donesene odluke.

2. Stavak 1. ne primjenjuje se na korištenje UI sustava za koje iznimke od obveze iz tog stavka ili njezina ograničenja proizlaze iz prava Unije ili nacionalnog prava u skladu s pravom Unije.
3. Ovaj se članak primjenjuje samo ako pravo iz stavka 1. nije na drugi način predviđeno na temelju prava Unije.

Članak 87.

Prijava povreda i zaštita prijavitelja povreda

Direktiva (EU) 2019/1937 primjenjuje se na prijave povreda ove Uredbe i zaštitu osoba koje prijavljuju takve povrede.

ODJELJAK 5.

NADZOR, ISTRAGE, IZVRŠAVANJE I PRAĆENJE

U VEZI S DOBAVLJAČIMA UI MODELÂ OPĆE NAMJENE

Članak 88.

Izvršavanje obveza dobavljača UI modelâ opće namjene

1. Komisija ima isključive ovlasti za nadzor i izvršavanje poglavlja V., uzimajući u obzir postupovna jamstva na temelju članka 94. Komisija provedbu tih zadaća povjerava Uredu za umjetnu inteligenciju, ne dovodeći u pitanje organizacijske ovlasti Komisije i podjelu nadležnosti između država članica i Unije na temelju Ugovorâ.

2. Ne dovodeći u pitanje članak 75. stavak 3., tijela za nadzor tržišta mogu od Komisije zatražiti da izvrši ovlasti utvrđene u ovom odjeljku ako je to potrebno i razmjerno kako bi im se pomoglo u ispunjavanju njihovih zadaća na temelju ove Uredbe.

Članak 89.

Mjere praćenja

1. Za potrebe obavljanja zadaća koje su mu dodijeljene na temelju ovog odjeljka Ured za umjetnu inteligenciju može poduzimati mjere potrebne za praćenje djelotvorne provedbe ove Uredbe i usklađenosti s njome od strane dobavljača UI modelâ opće namjene, među ostalim i njihova poštovanja odobrenih kodeksa prakse.
2. Dobavljači niže u lancu imaju pravo podnijeti pritužbu zbog navodne povrede ove Uredbe. Pritužba mora biti propisno obrazložena, a u njoj se navodi barem sljedeće:
 - (a) kontaktna točka dotičnog dobavljača UI modela opće namjene;
 - (b) opis relevantnih činjenica, dotične odredbe ove Uredbe i razlog zašto dobavljač niže u lancu smatra da je dotični dobavljač UI modela opće namjene počinio povredu ove Uredbe;
 - (c) sve ostale informacije koje dobavljač niže u lancu koji je podnio zahtjev smatra relevantnima, uključujući, prema potrebi, informacije prikupljene na vlastitu inicijativu.

Članak 90.

Upozorenja znanstvenog povjerenstva o sistemskim rizicima

1. Znanstveno povjerenstvo može Uredu za umjetnu inteligenciju dostaviti kvalificirano upozorenje ako ima razloga sumnjati na sljedeće:
 - (a) UI model opće namjene predstavlja konkretan utvrdiv rizik na razini Unije; ili
 - (b) UI model opće namjene ispunjava uvjete iz članka 51.
2. Slijedom takvog kvalificiranog upozorenja Komisija, putem Ureda za umjetnu inteligenciju i nakon što je obavijestila Vijeće za umjetnu inteligenciju, može izvršavati ovlasti utvrđene u ovom odjeljku u svrhu procjene tog pitanja. Ured za umjetnu inteligenciju obavještuje Vijeće za umjetnu inteligenciju o svim mjerama u skladu s člancima od 91. do 94.
3. Kvalificirano upozorenje mora biti propisno obrazloženo, a u njemu se navodi barem sljedeće:
 - (a) kontaktna točka dobavljača dotičnog UI modela opće namjene sa sistemskim rizikom;
 - (b) opis relevantnih činjenica i razloga za upozorenje znanstvenog povjerenstva;
 - (c) sve ostale informacije koje znanstveno povjerenstvo smatra relevantnima, uključujući, prema potrebi, informacije prikupljene na vlastitu inicijativu.

Članak 91.

Ovlast za zahtijevanje dokumentacije i informacija

1. Komisija može od dobavljača dotičnog UI modela opće namjene zahtijevati da dostavi dokumentaciju koju je dobavljač sastavio u skladu s člancima 53. i 55. ili sve dodatne informacije koje su potrebne u svrhu procjene usklađenosti dobavljača s ovom Uredbom.
2. Prije slanja zahtjeva za informacije Ured za umjetnu inteligenciju može pokrenuti strukturirani dijalog s dobavljačem UI modela opće namjene.
3. Na propisno obrazložen zahtjev znanstvenog povjerenstva Komisija može uputiti zahtjev za informacije dobavljaču UI modela opće namjene ako je pristup informacijama potreban i razmjeran za ispunjavanje zadaća znanstvenog povjerenstva u skladu s člankom 68. stavkom 2.
4. U zahtjevu za informacije navode se pravna osnova i svrha zahtjeva, preciziraju se informacije koje se zahtijevaju, određuje se rok u kojem se moraju dostaviti informacije i navode se novčane kazne predviđene u članku 101. za dostavljanje netočnih, nepotpunih ili obmanjujućih informacija.

5. Dobavljač dotičnog UI modela opće namjene ili njegov zastupnik dostavlja informacije obuhvaćene zahtjevom. U slučaju pravnih osoba, trgovačkih društava ili, ako dobavljač nema pravnu osobnost, osobe koje su ih na temelju zakona ili njihovih internih pravnih akata ovlaštene zastupati dostavljaju informacije obuhvaćene zahtjevom u ime dobavljača dotičnog UI modela opće namjene. Propisno ovlašteni odvjetnici mogu dostaviti informacije u ime svojih klijenata. Međutim, klijenti snose punu odgovornost ako su dostavljene informacije nepotpune, netočne ili obmanjujuće.

Članak 92.

Ovlast za provođenje evaluacija

1. Ured za umjetnu inteligenciju može, nakon savjetovanja s Vijećem za umjetnu inteligenciju, provoditi evaluacije dotičnog UI modela opće namjene radi sljedećeg:
 - (a) procjene usklađenosti dobavljača s obvezama na temelju ove Uredbe ako su informacije prikupljene na temelju članka 91. nedostatne; ili
 - (b) istrage sistemskih rizika na razini Unije u pogledu UI modelâ opće namjene sa sistemskim rizikom, posebice slijedom kvalificiranog upozorenja znanstvenog povjerenstva u skladu s člankom 90. stavkom 1. točkom (a).
2. Komisija može odlučiti imenovati neovisne stručnjake, među ostalim iz znanstvenog povjerenstva osnovanog na temelju članka 68., koji će biti zaduženi za provedbu evaluacija u njezino ime. Neovisni stručnjaci imenovani za tu zadaću moraju ispunjavati kriterije iz članka 68. stavka 2.

3. Za potrebe stavka 1. Komisija može zatražiti pristup dotičnom UI modelu opće namjene putem aplikacijskih programskih sučelja ili drugih odgovarajućih tehničkih sredstava i alata, uključujući izvorni kôd.
4. U zahtjevu za pristup navode se pravna osnova, svrha zahtjeva i razlozi za njegovo podnošenje, određuje se rok u kojem se mora omogućiti pristup i navode se novčane kazne predviđene u članku 101. ako se pristup ne omogući.
5. Dobavljač dotičnog UI modela opće namjene ili njegov zastupnik dostavlja informacije obuhvaćene zahtjevom. U slučaju pravnih osoba, trgovačkih društava ili, ako dobavljači nemaju pravnu osobnost, osobe koje su ih na temelju zakona ili njihovih internih pravnih akata ovlaštene zastupati omogućuju zatraženi pristup u ime dobavljača dotičnog UI modela opće namjene.
6. Komisija donosi provedbene akte kojima se utvrđuju detaljni aranžmani i uvjeti za evaluacije, uključujući detaljne aranžmane za uključivanje neovisnih stručnjaka i postupak za njihov odabir. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.
7. Prije nego što zatraži pristup dotičnom UI modelu opće namjene Ured za umjetnu inteligenciju može pokrenuti strukturirani dijalog s dobavljačem UI modela opće namjene kako bi prikupio više informacija o unutarnjem testiranju modela, unutarnjim zaštitnim mjerama za sprečavanje sistemskih rizika i drugim unutarnjim postupcima i mjerama koje je dobavljač poduzeo za ublažavanje takvih rizika.

Članak 93.

Ovlast za zahtijevanje mjera

1. Ako je to potrebno i primjereno, Komisija može od dobavljača zahtijevati sljedeće:
 - (a) da poduzmu odgovarajuće mjere za ispunjavanje obveza utvrđenih u člancima 53. i 54.;
 - (b) da provedu mjere za ublažavanje rizika ako je evaluacija provedena u skladu s člankom 92. rezultirala ozbiljnom i potkrijepljenom sumnjom na postojanje sistemskog rizika na razini Unije;
 - (c) da ograniče stavljanje modela na raspolaganje na tržištu, povuku ga ili opozovu.
2. Prije zahtijevanja mjere Ured za umjetnu inteligenciju može pokrenuti strukturirani dijalog s dobavljačem UI modela opće namjene.
3. Ako tijekom strukturiranog dijaloga iz stavka 2. dobavljač UI modela opće namjene sa sistemskim rizikom ponudi da će preuzeti obveze za provedbu mjera za ublažavanje sistemskog rizika na razini Unije, Komisija može odlukom odrediti da te obveze budu obvezujuće i navesti da nema daljnjih razloga za djelovanje.

Članak 94.

Postupovna prava gospodarskih subjekata UI modela opće namjene

Članak 18. Uredbe (EU) 2019/1020 primjenjuje se *mutatis mutandis* na dobavljače UI modela opće namjene, ne dovodeći u pitanje specifičnija postupovna prava predviđena u ovoj Uredbi.

Poglavlje X.

Kodeksi ponašanja i smjernice

Članak 95.

Kodeksi ponašanja za dobrovoljnu primjenu specifičnih zahtjeva

1. Ured za umjetnu inteligenciju i države članice potiču i olakšavaju izradu kodeksa ponašanja, uključujući povezane mehanizme upravljanja, namijenjenih poticanju dobrovoljne primjene pojedinih ili svih zahtjeva iz poglavlja III. odjeljka 2. na UI sustave koji nisu visokorizični, uzimajući u obzir dostupna tehnička rješenja i primjere najbolje prakse iz sektora koji omogućuju primjenu takvih zahtjeva.

2. Ured za umjetnu inteligenciju i države članice olakšavaju izradu kodeksa ponašanja koji se odnose na dobrovoljnu primjenu specifičnih zahtjeva na sve UI sustave, među ostalim od strane subjekata koji uvode sustav, na temelju jasnih ciljeva i ključnih pokazatelja uspješnosti za mjerenje ostvarenja tih ciljeva, koji uključuju, ali nisu ograničeni na sljedeće elemente:
- (a) primjenjive elemente predviđene u etičkim smjernicama Unije za pouzdanu umjetnu inteligenciju;
 - (b) procjenu učinka UI sustava na okolišnu održivost i njegovo svođenje na najmanju moguću mjeru, među ostalim u pogledu energetske učinkovitosti programiranja i tehnika za učinkovit dizajn, treniranje i korištenje umjetne inteligencije;
 - (c) promicanje pismenosti u području umjetne inteligencije, posebice za osobe koje se bave razvojem, radom i korištenjem umjetne inteligencije;
 - (d) olakšavanje uključivog i raznolikog dizajna UI sustava, među ostalim osnivanjem uključivih i raznolikih razvojnih timova i promicanjem sudjelovanja dionika u tom procesu;
 - (e) procjenu i sprečavanje negativnog učinka UI sustava na ranjive osobe ili skupine ranjivih osoba, među ostalim u pogledu pristupačnosti za osobe s invaliditetom, kao i na rodnu ravnopravnost.

3. Kodekse ponašanja mogu izraditi pojedinačni dobavljači UI sustava ili subjekti koji uvode te sustave ili organizacije koje ih zastupaju ili i ti dobavljači ili subjekti i te organizacije, među ostalim uz sudjelovanje svih zainteresiranih dionika i njihovih predstavničkih organizacija, uključujući organizacije civilnog društva i akademsku zajednicu. Kodeksi ponašanja mogu obuhvaćati jedan UI sustav ili više njih, uzimajući u obzir sličnost namjene relevantnih sustava.
4. Pri poticanju i olakšavanju izrade kodeksâ ponašanja Ured za umjetnu inteligenciju i države članice uzimaju u obzir posebne interese i potrebe MSP-ova, uključujući *start-up* poduzeća.

Članak 96.

Smjernice Komisije o provedbi ove Uredbe

1. Komisija izrađuje smjernice o praktičnoj provedbi ove Uredbe, a posebno o sljedećem:
 - (a) primjeni zahtjeva i obveza iz članaka od 8. do 15. i iz članka 25.;
 - (b) zabranjenim praksama iz članka 5.;
 - (c) praktičnoj provedbi odredaba o bitnoj izmjeni;
 - (d) praktičnoj provedbi obveza u pogledu transparentnosti utvrđenih u članku 50.;

- (e) detaljnim informacijama o odnosu ove Uredbe sa zakonodavstvom Unije o usklađivanju iz Priloga I., kao i s drugim relevantnim pravom Unije, među ostalim u pogledu dosljednosti u njihovu izvršavanju;
- (f) primjeni definicije UI sustava kako je utvrđena u članku 3. točki 1.

Pri izdavanju takvih smjernica Komisija posebnu pozornost posvećuje potrebama MSP-ova, uključujući *start-up* poduzeća, lokalnih tijela javne vlasti i sektora za koje postoji najveća vjerojatnost da će ova Uredba na njih utjecati.

U smjernicama iz prvog podstavka ovog stavka na odgovarajući način uzimaju se u obzir općepriznata najnovija dostignuća u području umjetne inteligencije, kao i relevantne usklađene norme i zajedničke specifikacije iz članaka 40. i 41. te usklađene norme ili tehničke specifikacije utvrđene na temelju prava Unije o usklađivanju.

2. Komisija na zahtjev država članica ili Ureda za umjetnu inteligenciju ili na vlastitu inicijativu ažurira prethodno donesene smjernice kada to smatra potrebnim.

Poglavlje XI.

Delegiranje ovlasti i postupak odbora

Članak 97.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.
2. Ovlast za donošenje delegiranih akata iz članka 6. stavaka 6. i 7., članka 7. stavaka 1. i 3., članka 11. stavka 3., članka 43. stavaka 5. i 6., članka 47. stavka 5., članka 51. stavka 3., članka 52. stavka 4. i članka 53. stavaka 5. i 6. dodjeljuje se Komisiji na razdoblje od pet godina počevši od ... [datum stupanja na snagu ove Uredbe]. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.
3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 6. stavaka 6. i 7., članka 7. stavaka 1. i 3., članka 11. stavka 3., članka 43. stavaka 5. i 6., članka 47. stavka 5., članka 51. stavka 3., članka 52. stavka 4. i članka 53. stavaka 5. i 6. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u *Službenom listu Europske unije* ili na kasniji datum naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.
5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.
6. Delegirani akt donesen na temelju članka 6. stavka 6. ili stavka 7., članka 7. stavka 1. ili stavka 3., članka 11. stavka 3., članka 43. stavka 5. ili stavka 6., članka 47. stavka 5., članka 51. stavka 3., članka 52. stavka 4. ili članka 53. stavka 5. ili stavka 6. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od tri mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za tri mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 98.

Postupak odbora

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.
2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

Poglavlje XII.

Sankcije

Članak 99.

Sankcije

1. U skladu s uvjetima utvrđenima u ovoj Uredbi, države članice utvrđuju pravila o sankcijama i drugim mjerama izvršavanja, koje također mogu uključivati upozorenja i nenovčane mjere, koje se primjenjuju na povrede ove Uredbe od strane operaterâ te poduzimaju sve potrebne mjere radi osiguranja njihove pravilne i djelotvorne provedbe, uzimajući pritom u obzir smjernice koje je Komisija izdala u skladu s člankom 96. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Njima se uzimaju u obzir interesi MSP-ova, uključujući *start-up* poduzeća, i njihova gospodarska održivost.
2. Države članice bez odgode, a najkasnije do datuma početka njihove primjene, obavješćuju Komisiju o pravilima o sankcijama i drugim mjerama izvršavanja iz stavka 1. te je bez odgode obavješćuju o svim njihovim naknadnim izmjenama.
3. Za nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5. izriču se upravne novčane kazne u iznosu do 35 000 000 EUR ili, ako je počinitelj poduzeće, do 7 % njegova ukupnog svjetskog godišnjeg prometa za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.

4. Za neusklađenost s jednom od sljedećih odredaba povezanih s operaterima ili prijavljenim tijelima, osim onih utvrđenih u članku 5., izriču se upravne novčane kazne u iznosu do 15 000 000 EUR ili, ako je počinitelj poduzeće, do 3 % njegova ukupnog svjetskog godišnjeg prometa za prethodnu financijsku godinu, ovisno o tome koji je iznos veći:
- (a) obvezama dobavljača na temelju članka 16.;
 - (b) obvezama ovlaštenih zastupnika na temelju članka 22.;
 - (c) obvezama uvoznika na temelju članka 23.;
 - (d) obvezama distributera na temelju članka 24.;
 - (e) obvezama subjekata koji uvode sustav na temelju članka 26.;
 - (f) zahtjevima i obvezama koji se odnose na prijavljena tijela na temelju članka 31., članka 33. stavaka 1., 3. i 4. ili članka 34.;
 - (g) obvezama u pogledu transparentnosti za dobavljače i subjekte koji uvode sustav na temelju članka 50.
5. Ako se prijavljenim tijelima ili nacionalnim nadležnim tijelima u odgovoru na zahtjev dostave netočne, nepotpune ili obmanjujuće informacije, izriču se upravne novčane kazne u iznosu do 7 500 000 EUR ili, ako je počinitelj poduzeće, do 1 % njegova ukupnog svjetskog godišnjeg prometa za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.
6. U slučaju MSP-ova, uključujući *start-up* poduzeća, maksimalna visina svake novčane kazne iz ovog članka odgovara postotku ili iznosu iz stavaka 3., 4. i 5., ovisno o tome koji je od ta dva iznosa manji.

7. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu u svakom pojedinačnom slučaju uzimaju se u obzir sve relevantne okolnosti specifične situacije te se, prema potrebi, pozornost posvećuje sljedećem:
- (a) prirodi, težini i trajanju povrede te njezinim posljedicama, uzimajući u obzir svrhu UI sustava te, prema potrebi, broj pogođenih osoba i razinu štete koju su pretrpjele;
 - (b) eventualnim upravnim novčanim kaznama koje su druga tijela za nadzor tržišta već izrekla istom operateru za istu povredu;
 - (c) eventualnim upravnim novčanim kaznama koje su druga tijela već izrekla istom operateru za povrede drugog prava Unije ili nacionalnog prava, ako su takve povrede posljedica iste aktivnosti ili propusta koji predstavljaju relevantnu povredu ove Uredbe;
 - (d) veličini, godišnjem prometu i tržišnom udjelu operatera koji je počinio povredu;
 - (e) svim ostalim otegotnim ili olakotnim čimbenicima primjenjivima na okolnosti slučaja, kao što su financijska korist ostvarena povredom ili gubici izbjegnuti, izravno ili neizravno, tom povredom;
 - (f) stupnju suradnje s nacionalnim nadležnim tijelima radi ispravljanja povrede i ublažavanja mogućih štetnih posljedica te povrede;

- (g) stupnju odgovornosti operatera, uzimajući u obzir tehničke i organizacijske mjere koje je proveo;
 - (h) načinu na koji su nacionalna nadležna tijela doznala za povredu, osobito je li i u kojoj mjeri operater obavijestio o povredi;
 - (i) tome je li povreda počinjena namjerno ili iz nepažnje;
 - (j) svim mjerama koje je operater poduzeo kako bi ublažio štetu koju su pretrpjele pogođene osobe.
8. Svaka država članica utvrđuje pravila o tome u kojoj se mjeri tijelima javne vlasti i javnim tijelima te države članice mogu izreći upravne novčane kazne.
9. Ovisno o pravnom sustavu država članica, pravila o upravnim novčanim kaznama mogu se primjenjivati tako da novčane kazne izriču nadležni nacionalni sudovi ili druga tijela, kako je primjenjivo u tim državama članicama. Primjena takvih pravila u tim državama članicama mora imati jednakovrijedan učinak.
10. Izvršavanje ovlasti na temelju ovog članka podliježe odgovarajućim postupovnim zaštitnim mjerama u skladu s pravom Unije i nacionalnim pravom, uključujući djelotvorna sudska pravna sredstva i zakonito postupanje.
11. Države članice svake godine izvješćuju Komisiju o upravnim novčanim kaznama koje su izrekle tijekom te godine, u skladu s ovim člankom, te o svim povezanim pravnim sporovima ili sudskim postupcima.

Članak 100.

Upravne novčane kazne za institucije, tijela, urede i agencije Unije

1. Europski nadzornik za zaštitu podataka može izreći upravne novčane kazne institucijama, tijelima, uredima i agencijama Unije obuhvaćenima područjem primjene ove Uredbe. Pri odlučivanju o izricanju upravne novčane kazne i o njezinu iznosu u svakom pojedinačnom slučaju uzimaju se u obzir sve relevantne okolnosti specifične situacije i dužna se pozornost posvećuje sljedećem:
 - (a) prirodi, težini i trajanju povrede te njezinim posljedicama, uzimajući u obzir svrhu dotičnog UI sustava te, prema potrebi, broj pogođenih osoba i razinu štete koju su pretrpjele;
 - (b) stupnju odgovornosti institucije, tijela, ureda ili agencije Unije, uzimajući u obzir tehničke i organizacijske mjere koje su proveli;
 - (c) svim mjerama koje su institucija, tijelo, ured ili agencija Unije poduzeli kako bi ublažili štetu koju su pretrpjele pogođene osobe;
 - (d) stupnju suradnje s Europskim nadzornikom za zaštitu podataka radi ispravljanja povrede i ublažavanja mogućih štetnih posljedica te povrede, uključujući usklađenost sa svim mjerama koje je Europski nadzornik za zaštitu podataka prethodno izrekao dotičnoj instituciji, tijelu, uredu ili agenciji Unije u vezi s istim predmetom;

- (e) svim sličnim prijašnjim povredama od strane dotične institucija, tijela, ureda ili agencije Unije;
 - (f) načinu na koji je Europski nadzornik za zaštitu podataka doznao za povredu, osobito jesu li i u kojoj mjeri institucija, tijelo, ured ili agencija Unije obavijestili o povredi;
 - (g) godišnjem proračunu institucije, tijela, ureda ili agencije Unije.
2. Za nepoštovanje zabrane praksi u području umjetne inteligencije iz članka 5. izriču se upravne novčane kazne u iznosu do 1 500 000 EUR.
 3. Za neusklađenost UI sustava s nekim od zahtjeva ili obveza na temelju ove Uredbe, osim onih utvrđeni u članku 5., izriču se upravne novčane kazne u iznosu do 750 000 EUR.
 4. Prije donošenja odluka u skladu s ovim člankom Europski nadzornik za zaštitu podataka pruža instituciji, tijelu, uredu ili agenciji Unije protiv kojih vodi postupak mogućnost da se očituju o mogućoj povredi. Europski nadzornik za zaštitu podataka svoje odluke temelji isključivo na elementima i okolnostima o kojima su se dotične stranke mogle očitovati. Eventualni podnositelji pritužbe moraju biti blisko uključeni u postupak.

5. U postupku se u potpunosti poštuje pravo dotičnih stranaka na obranu. Stranke imaju pravo na uvid u spis Europskog nadzornika za zaštitu podataka pod uvjetom da se poštuju legitimni interesi pojedinaca ili poduzeća da štite svoje osobne podatke ili poslovne tajne.
6. Sredstva prikupljena naplatom novčanih kazni iz ovog članka doprinos su općem proračunu Unije. Novčane kazne ne smiju utjecati na djelotvorno funkcioniranje institucije, tijela, ureda ili agencije Unije kojima je izrečena novčana kazna.
7. Europski nadzornik za zaštitu podataka jednom godišnje obavješćuje Komisiju o upravnim novčanim kaznama koje je izrekao na temelju ovog članka te o svim pravnim sporovima ili sudskim postupcima koje je pokrenuo.

Članak 101.

Novčane kazne za dobavljače UI modelâ opće namjene

1. Komisija može dobavljačima UI modelâ opće namjene izreći novčane kazne koje ne premašuju 3 % njihova ukupnog svjetskog prometa na godišnjoj razini u prethodnoj financijskoj godini ili 15 000 000 EUR, ovisno o tome koji je iznos veći, ako utvrdi da je dobavljač namjerno ili iz nepažnje učinio sljedeće:
 - (a) povrijedio je relevantne odredbe ove Uredbe;
 - (b) nije postupio u skladu sa zahtjevom za dokumentaciju ili informacije na temelju članka 91. ili je dostavio netočne, nepotpune ili obmanjujuće informacije;

- (c) nije postupio u skladu s mjerom zahtijevanom na temelju članka 93.;
- (d) Komisiji nije omogućio pristup UI modelu opće namjene ili UI modelu opće namjene sa sistemskim rizikom radi provedbe evaluacije na temelju članka 92.

Pri određivanju iznosa novčane kazne ili periodičnog penala u obzir se uzimaju priroda, težina i trajanje povrede, vodeći pritom na odgovarajući način računa o načelima proporcionalnosti i primjerenosti. Komisija također uzima u obzir obveze preuzete u skladu s člankom 93. stavkom 3. ili preuzete u relevantnim kodeksima prakse u skladu s člankom 56.

- 2. Prije donošenja odluke na temelju stavka 1. Komisija dostavlja svoje preliminarne nalaze dobavljaču UI modela opće namjene i pruža mu mogućnost da se očituje.
- 3. Novčane kazne izrečene u skladu s ovim člankom moraju biti učinkovite, proporcionalne i odvrćajuće.
- 4. Informacije o novčanim kaznama izrečenima na temelju ovog članka ujedno se prema potrebi priopćuju Vijeću za umjetnu inteligenciju.
- 5. Sud Europske unije ima neograničenu nadležnost za preispitivanje odluka Komisije kojima se određuje novčana kazna na temelju ovog članka. On izrečenu novčanu kaznu može ukinuti, smanjiti ili povećati.

6. Komisija donosi provedbene akte koji sadržavaju detaljne aranžmane i postupovne zaštitne mjere za postupke s obzirom na moguće donošenje odluka na temelju stavka 1. ovog članka. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 98. stavka 2.

Poglavlje XIII.

Završne odredbe

Članak 102.

Izmjena Uredbe (EZ) br. 300/2008

U članku 4. stavku 3. Uredbe (EZ) br. 300/2008 dodaje se sljedeći podstavak:

„Pri donošenju detaljnih mjera povezanih s tehničkim specifikacijama i postupcima za odobravanje i uporabu zaštitne opreme koje se odnose na sustave umjetne inteligencije u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 103.

Izmjena Uredbe (EU) br. 167/2013

U članku 17. stavku 5. Uredbe (EU) br. 167/2013 dodaje se sljedeći podstavak:

„Pri donošenju delegiranih akata na temelju prvog podstavka o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 104.

Izmjena Uredbe (EU) br. 168/2013

U članku 22. stavku 5. Uredbe (EU) br. 168/2013 dodaje se sljedeći podstavak:

„Pri donošenju delegiranih akata na temelju prvog podstavka o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 105.

Izmjena Direktive 2014/90/EU

U članku 8. Direktive 2014/90/EU dodaje se sljedeći stavak:

- „5. Kad je riječ o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺, Komisija pri obavljanju svojih aktivnosti na temelju stavka 1. i pri donošenju tehničkih specifikacija i ispitnih normi u skladu sa stavcima 2. i 3. u obzir uzima zahtjeve iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 106.

Izmjena Direktive (EU) 2016/797

U članku 5. Direktive (EU) 2016/797 dodaje se sljedeći stavak:

- „12. Pri donošenju delegiranih akata na temelju stavka 1. i provedbenih akata na temelju stavka 11. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 107.
Izmjena Uredbe (EU) 2018/858

U članku 5. Uredbe (EU) 2018/858 dodaje se sljedeći stavak:

- „4. Pri donošenju delegiranih akata na temelju stavka 3. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 108.
Izmjene Uredbe (EU) 2018/1139

Uredba (EU) 2018/1139 mijenja se kako slijedi:

1. u članku 17. dodaje se sljedeći stavak:

„3. Na dovodeći u pitanje stavak 2., pri donošenju provedbenih akata na temelju stavka 1. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”;

2. u članku 19. dodaje se sljedeći stavak:

„4. Pri donošenju delegiranih akata na temelju stavaka 1. i 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/...⁺⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

⁺⁺ SL: molimo umetnuti broj ove Uredbe (2021/0106(COD)).

3. u članku 43. dodaje se sljedeći stavak:

„4. Pri donošenju provedbenih akata na temelju stavaka 1. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/...⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

4. u članku 47. dodaje se sljedeći stavak:

„3. Pri donošenju delegiranih akata na temelju stavaka 1. i 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/...⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

5. u članku 57. dodaje se sljedeći podstavak:

„Pri donošenju tih provedbenih akata o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/...⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”;

6. u članku 58. dodaje se sljedeći stavak:

„3. Pri donošenju delegiranih akata na temelju stavaka 1. i 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/...⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.”.

⁺ SL: molimo umetnuti broj ove Uredbe (2021/0106(COD)).

Članak 109.

Izmjena Uredbe (EU) 2019/2144

U članku 11. Uredbe (EU) 2019/2144 dodaje se sljedeći stavak:

- „3. Pri donošenju provedbenih akata na temelju stavka 2. o sustavima umjetne inteligencije koji su sigurnosne komponente u smislu Uredbe (EU) 2024/... Europskog parlamenta i Vijeća⁺ u obzir se uzimaju zahtjevi iz poglavlja III. odjeljka 2. te uredbe.

* Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...).”.

⁺ SL: molimo u tekst umetnuti broj ove Uredbe (2021/0106(COD)) i dopuniti odgovarajuću bilješku.

Članak 110.

Izmjena Direktive (EU) 2020/1828

U Prilogu I. Direktivi (EU) 2020/1828 Europskog parlamenta i Vijeća⁵⁸ dodaje se sljedeća točka:

„68. Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ...⁺ o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, ..., ELI: ...)”.

Članak 111.

UI sustavi koji su već stavljeni na tržište ili u upotrebu i UI modeli opće namjene koji su već stavljeni na tržište

1. Ne dovodeći u pitanje primjenu članka 5. kako je predviđena u članku 113. stavku 3. točki (a), UI sustavi koji su komponente opsežnih informacijskih sustava uspostavljenih pravnim aktima iz Priloga X. i koji su stavljeni na tržište ili u upotrebu prije ... [36 mjeseci od datuma stupanja na snagu ove Uredbe] usklađuju se s ovom Uredbom do 31. prosinca 2030.

⁵⁸ Direktiva (EU) 2020/1828 Europskog parlamenta i Vijeća od 25. studenoga 2020. o predstavničkim tužbama za zaštitu kolektivnih interesa potrošača i stavljanju izvan snage Direktive 2009/22/EZ (SL L 409, 4.12.2020., str. 1.).

⁺ SL: molimo umetnuti u tekst datum i broj ove uredbe (2021/0106(COD)).

Zahtjevi utvrđeni u ovoj Uredbi uzimaju se u obzir pri evaluaciji svakog opsežnog informacijskog sustava uspostavljenog pravnim aktima iz Priloga X. koju treba provesti kako je predviđeno u tim pravnim aktima i onda kada se ti pravni akti zamjenjuju ili mijenjaju.

2. Ne dovodeći u pitanje primjenu članka 5. kako je predviđena u članku 113. stavku 3. točki (a), ova se Uredba primjenjuje na operatere visokorizičnih UI sustava, osim sustava iz stavka 1. ovog članka, koji su stavljeni na tržište ili u upotrebu prije... [24 mjeseca od datuma stupanja na snagu ove Uredbe] samo ako se nakon tog datuma znatno promijeni dizajn tih sustava. U svakom slučaju, dobavljači visokorizičnih UI sustava i subjekti koji ih uvode, koji su namijenjeni korištenju od strane tijela javne vlasti, poduzimaju potrebne korake kako bi ispunili zahtjeve i obveze iz ove Uredbe do ... [šest godina od datuma stupanja na snagu ove Uredbe].
3. Dobavljači UI modela opće namjene koji su stavljeni na tržište prije ... [12 mjeseci od datuma stupanja na snagu ove Uredbe] poduzimaju potrebne korake kako bi ispunili obveze utvrđene u ovoj Uredbi do ... [36 mjeseci od datuma stupanja na snagu ove Uredbe].

Članak 112.

Evaluacija i preispitivanje

1. Komisija jednom godišnje nakon stupanja na snagu ove Uredbe i do kraja razdoblja delegiranja ovlasti utvrđenog u članku 97. procjenjuje potrebu za izmjenom popisa iz Priloga III. i popisa zabranjenih praksi u području umjetne inteligencije utvrđenog u članku 5. Komisija zaključke te procjene podnosi Europskom parlamentu i Vijeću.
2. Komisija do ... [četiri godine od datuma stupanja na snagu ove Uredbe] i svake četiri godine nakon toga provodi evaluaciju te izvješćuje Europski parlament i Vijeće o sljedećem:
 - (a) potrebi za izmjenama radi proširenja postojećih kategorija područja ili dodavanja novih područja u Prilog III.;
 - (b) izmjenama popisa UI sustava za koje su potrebne dodatne mjere transparentnosti iz članka 50.;
 - (c) izmjenama radi povećanja djelotvornosti sustava nadzora i upravljanja.

3. Komisija do ... [pet godina od datuma stupanja na snagu ove Uredbe] i svake četiri godine nakon toga Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe. Izvješće uključuje ocjenu u vezi sa strukturom izvršavanja i mogućom potrebom da agencija Unije otkloni utvrđene nedostatke. Na temelju nalaza tom se izvješću, prema potrebi, prilaže prijedlog za izmjenu ove Uredbe. Ta se izvješća objavljuju.
4. U izvješćima iz stavka 2. posebna se pozornost posvećuje sljedećem:
- (a) stanju financijskih, tehničkih i ljudskih resursa nacionalnih nadležnih tijela za djelotvorno obavljanje zadaća koje su im dodijeljene na temelju ove Uredbe;
 - (b) stanju sankcija, a posebno upravnih novčanih kazni iz članka 99. stavka 1. koje države članice primjenjuju za povrede ove Uredbe;
 - (c) donesenim usklađenim normama i zajedničkim specifikacijama razvijenima kao potpora ovoj Uredbi;
 - (d) broju poduzeća koja ulaze na tržište nakon početka primjene ove Uredbe i koliko je među njima MSP-ova.

5. Komisija do ... [četiri godine od datuma stupanja na snagu ove Uredbe] evaluira funkcioniranje Ureda za umjetnu inteligenciju, jesu li Uredu za umjetnu inteligenciju dodijeljene dostatne ovlasti i nadležnosti za ispunjavanje njegovih zadaća i bi li za pravilnu provedbu i izvršavanje ove Uredbe bilo relevantno i potrebno osnažiti Ured za umjetnu inteligenciju i njegove nadležnosti u području izvršavanja te povećati njegove resurse. Komisija podnosi izvješće o svojoj evaluaciji Europskom parlamentu i Vijeću.
6. Komisija do ... [četiri godine od datuma stupanja na snagu ove Uredbe] i svake četiri godine nakon toga podnosi izvješće o preispitivanju napretka u razvoju normizacijskih dokumenata o energetske učinkovitom razvoju UI modela opće namjene te procjenjuje potrebu za daljnjim mjerama ili djelovanjem, uključujući obvezujuće mjere ili djelovanje. To se izvješće podnosi Europskom parlamentu i Vijeću i objavljuje.
7. Komisija do ... [četiri godine od datuma stupanja na snagu ove Uredbe] i svake tri godine nakon toga evaluira učinak i djelotvornost dobrovoljnih kodeksa ponašanja namijenjenih poticanju primjene zahtjeva utvrđenih u poglavlju III. odjeljku 2. za UI sustave koji nisu visokorizični i eventualno drugih dodatnih zahtjeva za UI sustave koji nisu visokorizični, među ostalim u pogledu okolišne održivosti.
8. Za potrebe stavaka od 1. do 7. Vijeće za umjetnu inteligenciju, države članice i nacionalna nadležna tijela Komisiji dostavljaju informacije na njezin zahtjev i bez nepotrebne odgode.

9. Pri provedbi evaluacija i preispitivanja iz stavaka od 1. do 7. Komisija uzima u obzir stajališta i zaključke Vijeća za umjetnu inteligenciju, Europskog parlamenta, Vijeća i drugih relevantnih tijela ili izvora.
10. Komisija prema potrebi podnosi odgovarajuće prijedloge radi izmjene ove Uredbe, posebno uzimajući u obzir razvoj tehnologije i učinke UI sustavâ na zdravlje i sigurnost te na temeljna prava, i s obzirom na napredak informacijskog društva.
11. Radi usmjeravanja evaluacija i preispitivanja iz stavaka od 1. do 7. ovog članka Ured za umjetnu inteligenciju obvezuje se razviti objektivnu i participativnu metodologiju za evaluaciju razine rizika na temelju kriterija navedenih u relevantnim člancima i za uključivanje novih sustava na sljedeće:
- (a) popis utvrđen u Prilogu III., uključujući proširenje postojećih kategorija područja ili dodavanje novih kategorija područja u taj prilog;
 - (b) popis zabranjenih praksi utvrđen u članku 5.; i
 - (c) popis UI sustava za koje su potrebne dodatne mjere transparentnosti na temelju članka 50.
12. Pri svakoj izmjeni ove Uredbe na temelju stavka 10. ili relevantnih delegiranih akata ili provedbenih akata koja se odnosi na sektorsko zakonodavstvo Unije o usklađivanju navedeno u odjeljku B Priloga I. u obzir se uzimaju regulatorne posebnosti svakog sektora i postojeći mehanizmi upravljanja, ocjenjivanja sukladnosti i izvršenja te tijela koja su njime utvrđena.

13. Komisija do ... [sedam godina od datuma stupanja na snagu ove Uredbe] ocjenjuje izvršavanje ove Uredbe i o tome izvješćuje Europski parlament, Vijeće te Europski gospodarski i socijalni odbor, uzimajući u obzir prve godine primjene ove Uredbe. Na temelju zaključaka tom se izvješću prema potrebi prilaže prijedlog za izmjenu ove Uredbe u vezi sa strukturom izvršavanja i potrebom da agencija Unije otkloni utvrđene nedostatke.

Članak 113.

Stupanje na snagu i primjena

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od ... [24 mjeseca od datuma stupanja na snagu ove Uredbe].

Međutim:

- (a) poglavlja I. i II. primjenjuju se od ... [šest mjeseci od datuma stupanja na snagu ove Uredbe];
- (b) poglavlje III. odjeljak 4., poglavlje V., poglavlje VII. i poglavlje XII. te članak 78. primjenjuju se od ... [12 mjeseci od datuma stupanja na snagu ove Uredbe], uz iznimku članka 101.;

- (c) članak 6. stavak 1. i odgovarajuće obveze iz ove Uredbe primjenjuju se od ... [36 mjeseci od datuma stupanja na snagu ove Uredbe].

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu

Za Europski parlament

Predsjednica

Za Vijeće

Predsjednik/Predsjednica

PRILOG I.

Popis zakonodavstva Unije o usklađivanju

Odjeljak A. Popis zakonodavstva Unije o usklađivanju na temelju novog zakonodavnog okvira

1. Direktiva 2006/42/EZ Europskog parlamenta i Vijeća od 17. svibnja 2006. o strojevima o izmjeni Direktive 95/16/EZ (SL L 157, 9.6.2006., str. 24.);
2. Direktiva 2009/48/EZ Europskog parlamenta i Vijeća od 18. lipnja 2009. o sigurnosti igračaka (SL L 170, 30.6.2009., str. 1.);
3. Direktiva 2013/53/EU Europskog parlamenta i Vijeća od 20. studenoga 2013. o rekreacijskim plovilima i osobnim plovilima na vodomlazni pogon i o stavljanju izvan snage Direktive Vijeća 94/25/EZ (SL L 354, 28.12.2013., str. 90.);
4. Direktiva 2014/33/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na dizala i sigurnosne komponente za dizala (SL L 96, 29.3.2014., str. 251.);
5. Direktiva 2014/34/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o usklađivanju zakonodavstava država članica u odnosu na opremu i zaštitne sustave namijenjene za uporabu u potencijalno eksplozivnim atmosferama (SL L 96, 29.3.2014., str. 309.);

6. Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62.);
7. Direktiva 2014/68/EU Europskog parlamenta i Vijeća od 15. svibnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje na tržištu tlačne opreme (SL L 189, 27.6.2014., str. 164.);
8. Uredba (EU) 2016/424 Europskog parlamenta i Vijeća od 9. ožujka 2016. o žičarama i stavljanju izvan snage Direktive 2000/9/EZ (SL L 81, 31.3.2016., str. 1.);
9. Uredba (EU) 2016/425 Europskog parlamenta i Vijeća od 9. ožujka 2016. o osobnoj zaštitnoj opremi i o stavljanju izvan snage Direktive Vijeća 89/686/EEZ (SL L 81, 31.3.2016., str. 51.);
10. Uredba (EU) 2016/426 Europskog parlamenta i Vijeća od 9. ožujka 2016. o aparatima na plinovita goriva i stavljanju izvan snage Direktive 2009/142/EZ (SL L 81, 31.3.2016., str. 99.);
11. Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1.);

12. Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176.).

Odjeljak B. Popis ostalog zakonodavstva Unije o usklađivanju

13. Uredba (EZ) br. 300/2008 Europskog parlamenta i Vijeća od 11. ožujka 2008. o zajedničkim pravilima u području zaštite civilnog zračnog prometa i stavljanju izvan snage Uredbe (EZ) br. 2320/2002 (SL L 97, 9.4.2008., str. 72.);
14. Uredba (EU) br. 168/2013 Europskog parlamenta i Vijeća od 15. siječnja 2013. o homologaciji i nadzoru tržišta vozila na dva ili tri kotača i četverocikala (SL L 60, 2.3.2013., str. 52.);
15. Uredba (EU) br. 167/2013 Europskog parlamenta i Vijeća od 5. veljače 2013. o homologaciji i nadzoru tržišta traktora za poljoprivredu i šumarstvo (SL L 60, 2.3.2013., str. 1.);
16. Direktiva 2014/90/EU Europskog parlamenta i Vijeća od 23. srpnja 2014. o pomorskoj opremi i stavljanju izvan snage Direktive Vijeća 96/98/EZ (SL L 257, 28.8.2014., str. 146.);
17. Direktiva (EU) 2016/797 Europskog parlamenta i Vijeća od 11. svibnja 2016. o interoperabilnosti željezničkog sustava u Europskoj uniji (SL L 138, 26.5.2016., str. 44.);

18. Uredba (EU) 2018/858 Europskog parlamenta i Vijeća od 30. svibnja 2018. o homologaciji i nadzoru tržišta motornih vozila i njihovih prikolica te sustavâ, sastavnih dijelova i zasebnih tehničkih jedinica namijenjenih za takva vozila, o izmjeni uredaba (EZ) br. 715/2007 i (EZ) br. 595/2009 te o stavljanju izvan snage Direktive 2007/46/EZ (SL L 151, 14.6.2018., str. 1.);
19. Uredba (EU) 2019/2144 Europskog parlamenta i Vijeća od 27. studenoga 2019. o zahtjevima za homologaciju tipa za motorna vozila i njihove prikolice te za sustave, sastavne dijelove i zasebne tehničke jedinice namijenjene za takva vozila, u pogledu njihove opće sigurnosti te zaštite osoba u vozilima i nezaštićenih sudionika u cestovnom prometu, o izmjeni Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća i stavljanju izvan snage uredbi (EZ) br. 78/2009, (EZ) br. 79/2009 i (EZ) br. 661/2009 Europskog parlamenta i Vijeća i uredbi Komisije (EZ) br. 631/2009, (EU) br. 406/2010, (EU) br. 672/2010, (EU) br. 1003/2010, (EU) br. 1005/2010, (EU) br. 1008/2010, (EU) br. 1009/2010, (EU) br. 19/2011, (EU) br. 109/2011, (EU) br. 458/2011, (EU) br. 65/2012, (EU) br. 130/2012, (EU) br. 347/2012, (EU) br. 351/2012, (EU) br. 1230/2012 i (EU) 2015/166 (SL L 325, 16.12.2019., str. 1.);

20. Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.), kada je riječ o projektiranju, proizvodnji i stavljanju na tržište zrakoplova iz članka 2. stavka 1. točaka (a) i (b), u vezi s bespilotnim zrakoplovima i njihovim motorima, propelerima, dijelovima i opremi za daljinsko upravljanje tim zrakoplovima.
-

PRILOG II.

Popis kaznenih djela iz članka 5. stavka 1. prvog podstavka točke (h) podtočke iii.

Kaznena djela iz članka 5. stavka 1. prvog podstavka točke (h) podtočke iii.:

- terorizam,
- trgovina ljudima,
- seksualno iskorištavanje djece i dječja pornografija,
- nezakonita trgovina opojnim drogama ili psihotropnim tvarima,
- nezakonita trgovina oružjem, streljivom ili eksplozivima,
- ubojstvo, teška tjelesna ozljeda,
- nezakonita trgovina ljudskim organima ili tkivom,
- nezakonita trgovina nuklearnim ili radioaktivnim materijalima,
- otmica, protupravno oduzimanje slobode ili uzimanje talaca,
- kaznena djela iz nadležnosti Međunarodnog kaznenog suda,
- protupravno oduzimanje zrakoplova ili brodova,

- silovanje,
 - kazneno djelo protiv okoliša,
 - organizirana ili oružana pljačka,
 - sabotaža,
 - sudjelovanje u zločinačkoj organizaciji uključenoj u jednoj od navedenih kaznenih djela ili više njih.
-

PRILOG III.

Visokorizični UI sustavi iz članka 6. stavka 2.

Visokorizični UI sustavi u skladu s člankom 6. stavkom 2. jesu UI sustavi u bilo kojem od sljedećih područja:

1. Biometrija, ako je njezino korištenje dopušteno na temelju relevantnog prava Unije ili nacionalnog prava:
 - (a) sustavi za daljinsku biometrijsku identifikaciju.

To ne uključuje UI sustave namijenjene za biometrijsku provjeru čija je jedina svrha potvrditi da je određena fizička osoba doista ona osoba kojom se predstavlja;
 - (b) UI sustavi namijenjeni za biometrijsku kategorizaciju, u skladu s osjetljivim ili zaštićenim atributima ili karakteristikama na temelju zaključivanja o tim atributima ili značajkama;
 - (c) UI sustavi namijenjeni za prepoznavanje emocija.
2. Kritična infrastruktura: UI sustavi namijenjeni za korištenje kao sigurnosne komponente za upravljanje kritičnom digitalnom infrastrukturom, cestovnim prometom ili opskrbom vodom, plinom, grijanjem ili električnom energijom te za njihov rad.

3. Obrazovanje i strukovno osposobljavanje:

- (a) UI sustavi namijenjeni za odlučivanje o pristupu ili upisu ili za razvrstavanje fizičkih osoba u ustanove ili programe za obrazovanje i strukovno osposobljavanje na svim razinama;
- (b) UI sustavi namijenjeni za evaluaciju ishoda učenja, među ostalim kad se ti ishodi upotrebljavaju za usmjeravanje procesa učenja fizičkih osoba u ustanovama za obrazovanje i strukovno osposobljavanje na svim razinama;
- (c) UI sustavi namijenjeni za upotrebu u svrhu procjene odgovarajuće razine obrazovanja koju će pojedinci primiti ili kojoj će moći pristupiti, u kontekstu ili unutar ustanova za obrazovanje i strukovno osposobljavanje na svim razinama;
- (d) UI sustavi namijenjeni za praćenje i otkrivanje zabranjenog postupanja učenika tijekom testiranja u kontekstu ili unutar ustanova za obrazovanje i strukovno osposobljavanje na svim razinama.

4. Zapošljavanje, kadrovsko upravljanje i pristup samozapošljavanju:

- (a) UI sustavi namijenjeni za zapošljavanje ili odabir fizičkih osoba, posebno za postavljanje ciljanih oglasa za posao, za analizu i filtriranje prijava za posao te za evaluaciju kandidata;

- (b) UI sustavi namijenjeni za donošenje odluka koje utječu na uvjete radnog odnosa, promaknuće ili otkazivanje radnih ugovornih odnosa, za dodjelu zadataka na osnovi individualnog ponašanja ili osobnih obilježja odnosno karakteristika te za praćenje i evaluaciju učinkovitosti i ponašanja osoba u takvim odnosima.

5. Pristup osnovnim privatnim uslugama te osnovnim javnim uslugama i naknadama i njihovo korištenje:

- (a) UI sustavi namijenjeni za korištenje od strane tijela javne vlasti ili u njihovo ime za evaluaciju prihvatljivosti fizičkih osoba za osnovne naknade i usluge javne pomoći, uključujući zdravstvene usluge, te za dodjeljivanje, smanjenje, ukidanje ili povrat takvih naknada i usluga;
- (b) UI sustavi namijenjeni za evaluaciju kreditne sposobnosti fizičkih osoba ili utvrđivanje njihova kreditnog rejtinga, uz iznimku UI sustava koji se upotrebljavaju za otkrivanje financijskih prijevara;
- (c) UI sustavi namijenjeni za procjenu rizika i određivanje cijena u odnosu na fizičke osobe u slučaju životnog i zdravstvenog osiguranja;
- (d) UI sustavi namijenjeni za evaluaciju i klasifikaciju hitnih poziva fizičkih osoba ili za dispečiranje ili određivanje prioriteta pri dispečiranju hitnih službi, uključujući policiju, vatrogasce i medicinsku pomoć, kao i sustave za trijažu pacijenata u pružanju hitne skrbi.

6. Kazneni progon, ako je njihovo korištenje dopušteno na temelju relevantnog prava Unije ili nacionalnog prava:
- (a) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona ili u njihovo ime za procjenu rizika fizičke osobe da postane žrtva kaznenih djela;
 - (b) UI sustavi namijenjeni za upotrebu od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona kao poligrafi ili slični alati;
 - (c) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona za evaluaciju pouzdanosti dokaza tijekom istrage ili progona kaznenih djela;
 - (d) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona za procjenu rizika fizičke osobe do počini ili ponovno počini kazneno djelo ne samo na osnovi izrade profila fizičkih osoba kako je navedeno u članku 3. točki 4. Direktive (EU) 2016/680 ili za procjenu osobina i karakteristika ili prethodnog kriminalnog ponašanja fizičkih osoba ili skupina;

- (e) UI sustavi namijenjeni za korištenje od strane tijela kaznenog progona ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za potporu tijelima kaznenog progona za izradu profila fizičkih osoba kako je navedeno u članku 3. točki 4. Direktive (EU) 2016/680 tijekom otkrivanja, istrage ili progona kaznenih djela.

7. Migracije, azil i upravljanje nadzorom državne granice, ako je njihovo korištenje dopušteno na temelju relevantnog prava Unije ili nacionalnog prava:

- (a) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije kao poligrafi ili slični alati;
- (b) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za procjenu rizika, uključujući rizik za sigurnost, rizik od nezakonitih migracija ili rizik za zdravlje, koji predstavlja fizička osoba koja namjerava ući ili je ušla na državno područje države članice;
- (c) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije za pomoć nadležnim tijelima javne vlasti u razmatranju zahtjeva za azil, viza ili boravišnih dozvola i povezanih pritužbi u pogledu prihvatljivosti fizičkih osoba koje podnose zahtjev za određeni status, uključujući povezane procjene pouzdanosti dokaza;

- (d) UI sustavi namijenjeni za korištenje od strane nadležnih tijela javne vlasti ili u njihovo ime ili od strane institucija, tijela, ureda ili agencija Unije, u kontekstu migracija, azila ili upravljanja nadzorom državne granice, u svrhu otkrivanja, prepoznavanja ili identifikacije fizičkih osoba, uz iznimku provjere putnih isprava.

8. Sudovanje i demokratski procesi:

- (a) UI sustavi namijenjeni za korištenje od strane pravosudnih tijela ili u njihovo ime za pomoć pravosudnom tijelu u istraživanju i tumačenju činjenica i prava te primjeni prava na konkretan skup činjenica ili za upotrebu na sličan način u alternativnom rješavanju sporova;
- (b) UI sustavi namijenjeni za utjecanje na ishod izbora ili referenduma ili na ponašanje fizičkih osoba pri glasovanju na izborima ili referendumima. To ne uključuje UI sustave čijim izlaznim podacima fizičke osobe nisu izravno izložene, kao što su alati koji se upotrebljavaju za organizaciju, optimizaciju i strukturiranje političkih kampanja s administrativnog ili logističkog stajališta.

PRILOG IV.

Tehnička dokumentacija iz članka 11. stavka 1.

Tehnička dokumentacija iz članka 11. stavka 1. sadržava barem sljedeće informacije, ovisno o tome što je primjenjivo na dotični UI sustav:

1. opći opis UI sustava, uključujući:
 - (a) njegovu namjenu, ime dobavljača i verziju sustava koja odražava njegovu povezanost s prethodnim verzijama;
 - (b) način na koji je UI sustav u interakciji s hardverom ili softverom, među ostalim s drugim UI sustavima koji nisu dio samog UI sustava, ili način na koji se može upotrijebiti za takvu interakciju, ako je primjenjivo;
 - (c) verzije relevantnog softvera ili ugrađenog softvera i sve zahtjeve povezane s ažuriranjem verzija;
 - (d) opis svih oblika u kojima se UI sustav stavlja na tržište ili u upotrebu, kao što su softverski paketi ugrađeni u hardver, preuzimanja ili aplikacijska programska sučelja;
 - (e) opis hardvera na kojem bi UI sustav trebao raditi;
 - (f) ako je UI sustav komponenta proizvoda, fotografije ili ilustracije koje prikazuju vanjske značajke, oznake i unutarnju strukturu tih proizvoda;

- (g) osnovni opis korisničkog sučelja koje se pruža subjektu koji uvodi sustav;
- (h) upute za korištenje namijenjene subjektu koji uvodi sustav i osnovni opis korisničkog sučelja koje se pruža subjektu koji uvod sustav, ako je primjenjivo;

2. detaljan opis elemenata UI sustava i postupka njegova razvoja, uključujući:

- (a) metode i korake provedene u razvoju UI sustava, uključujući, ako je to relevantno, upotrebu prethodno treniranih sustava ili alata trećih strana i način na koji ih je dobavljač upotrijebio, integrirao ili izmijenio;
- (b) specifikacije dizajna sustava, odnosno opću logiku UI sustava i algoritama; najvažnije odabire u pogledu dizajna, uključujući obrazloženja i pretpostavke, među ostalim u vezi s osobama ili skupinama osoba u vezi s kojima se sustav namjerava upotrebljavati; glavne klasifikacijske odabire; informacije o tome što bi sustav svojim dizajnom trebao optimizirati i relevantnost različitih parametara; opis očekivanih izlaznih podataka sustava i njihove kvalitete; odluke o eventualnim kompromisima u pogledu tehničkih rješenja donesenima radi ispunjavanja zahtjeva iz poglavlja III. odjeljka 2.;
- (c) opis arhitekture sustava u kojem se objašnjava kako se softverske komponente međusobno nadopunjuju ili potpomažu te kako su integrirane u cjelokupnu obradu; računalne resurse upotrijebljene za razvoj, treniranje, testiranje i validaciju UI sustava;

- (d) ako je to relevantno, zahtjeve u pogledu podataka u smislu tablica s opisom metodologija i tehnika treniranja te upotrijebljenih skupova podataka za treniranje, uključujući opći opis tih skupova podataka i informacije o njihovu podrijetlu, sadržaju i glavnim karakteristikama; način na koji su podaci dobiveni i odabrani; postupke označivanja (npr. za nadzirano učenje), metodologije čišćenja podataka (npr. otkrivanje netipičnih vrijednosti);
- (e) procjenu mjera ljudskog nadzora potrebnih u skladu s člankom 14., uključujući procjenu tehničkih mjera potrebnih kako bi se subjektima koji uvode sustav olakšalo tumačenje izlaznih podataka UI sustava, u skladu s člankom 13. stavkom 3. točkom (d);
- (f) ako je primjenjivo, detaljan opis unaprijed određenih promjena UI sustava i njegove učinkovitosti, zajedno sa svim relevantnim informacijama o tehničkim rješenjima primijenjenima radi osiguravanja kontinuirane usklađenosti UI sustava s relevantnim zahtjevima iz poglavlja III. odjeljka 2.;
- (g) primijenjene postupke validacije i testiranja, uključujući informacije o podacima upotrijebljenima za validaciju i testiranje te njihovim glavnim karakteristikama; parametre upotrijebljene za mjerenje točnosti, otpornosti i usklađenosti s drugim relevantnim zahtjevima iz poglavlja III. odjeljka 2., kao i potencijalne diskriminirajuće učinke; evidenciju događaja tijekom testiranja i sva izvješća o testiranju s datumom i potpisom odgovornih osoba, među ostalim u vezi s unaprijed određenim promjenama iz točke (f);
- (h) uspostavljene mjere u području kibernetičke sigurnosti;

3. detaljne informacije o praćenju, funkcioniranju i kontroli UI sustava, posebno u pogledu sljedećeg: njegovih sposobnosti i ograničenja u radu, uključujući stupnjeve točnosti za konkretne osobe ili skupine osoba na kojima se sustav namjerava upotrebljavati te ukupnu očekivanu razinu točnosti u odnosu na namjenu sustava; predvidljivih neplaniranih ishoda i izvora rizika za zdravlje i sigurnost, temeljna prava i u pogledu diskriminacije s obzirom na namjenu UI sustava; mjera ljudskog nadzora potrebnih u skladu s člankom 14., uključujući tehničke mjere uspostavljene kako bi se subjektima koji uvode sustav olakšalo tumačenje izlaznih podataka UI sustava; specifikacije ulaznih podataka, prema potrebi;
4. opis primjerenosti parametara učinkovitosti za određeni UI sustav;
5. detaljan opis sustava upravljanja rizikom u skladu s člankom 9.;
6. opis svih relevantnih promjena koje je dobavljač unio u sustav tijekom njegova životnog ciklusa;
7. popis u cijelosti ili djelomično primijenjenih usklađenih normi na koje su objavljena upućivanja u *Službenom listu Europske unije*; ako nisu primijenjene takve usklađene norme, detaljan opis rješenja koja su primijenjenima radi ispunjavanja zahtjeva iz poglavlja III. odjeljka 2., uključujući popis drugih primijenjenih relevantnih normi i tehničkih specifikacija;
8. primjerak EU izjave o sukladnosti iz članka 47.;
9. detaljan opis sustava uspostavljenog za evaluaciju učinkovitosti UI sustava u fazi nakon stavljanja na tržište u skladu s člankom 72., uključujući plan praćenja nakon stavljanja na tržište iz članka 72. stavka 3.

PRILOG V.

EU izjava o sukladnosti

EU izjava o sukladnosti iz članka 47. sadržava sve sljedeće informacije:

1. ime i vrstu UI sustava te sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;
2. ime i adresu dobavljača ili, kada je to primjenjivo, njegova ovlaštenog zastupnika;
3. izjavu da je za izdavanje EU izjave o sukladnosti iz članka 47. odgovoran isključivo dobavljač;
4. izjavu da je UI sustav sukladan s ovom Uredbom i, ako je primjenjivo, sa svim drugim relevantnim pravom Unije kojim je predviđeno izdavanje EU izjave o sukladnosti iz članka 47.;
5. ako UI sustav obuhvaća obradu osobnih podataka, izjavu da je taj UI sustav usklađen s uredbama (EU) 2016/679 i (EU) 2018/1725 te Direktivom (EU) 2016/680;
6. upućivanja na sve primijenjene relevantne usklađene norme ili druge zajedničke specifikacije u odnosu na koje se izjavljuje sukladnost;

7. ako je primjenjivo, ime i identifikacijski broj prijavljenog tijela, opis provedenog postupka ocjenjivanja sukladnosti te identifikacijsku oznaku izdane potvrde;
 8. mjesto i datum izdavanja izjave, ime i funkciju osobe koja ju je potpisala, uključujući navod za koga ili u čije ime je potpisana, te potpis.
-

PRILOG VI.

Postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole

1. Postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole postupak je ocjenjivanja sukladnosti na temelju točaka 2., 3. i 4.
 2. Dobavljač provjerava je li uveden sustav upravljanja kvalitetom usklađen sa zahtjevima iz članka 17.
 3. Dobavljač pregledava informacije iz tehničke dokumentacije kako bi ocijenio usklađenost UI sustava s relevantnim temeljnim zahtjevima iz poglavlja III. odjeljka 2.
 4. Osim toga, dobavljač provjerava jesu li postupak dizajniranja i razvoja UI sustava te njegovo praćenje nakon stavljanja na tržište iz članka 72. u skladu s tehničkom dokumentacijom.
-

PRILOG VII.

Sukladnost na temelju ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije

1. Uvod

Sukladnost na temelju ocjenjivanja sustava upravljanja kvalitetom i ocjenjivanja tehničke dokumentacije postupak je ocjenjivanja sukladnosti na temelju točaka od 2. do 5.

2. Pregled

Odobreni sustav upravljanja kvalitetom za dizajniranje, razvoj i testiranje UI sustavâ na temelju članka 17. ispituje se u skladu s točkom 3. i podliježe nadzoru kako je utvrđeno u točki 5. Tehnička dokumentacija UI sustava pregledava se u skladu s točkom 4.

3. Sustav upravljanja kvalitetom

3.1. Zahtjev dobavljača sadržava:

- (a) ime i adresu dobavljača te, ako je zahtjev podnio ovlašteni zastupnik, i njegovo ime te adresu;
- (b) popis UI sustava obuhvaćenih istim sustavom upravljanja kvalitetom;
- (c) tehničku dokumentaciju za svaki UI sustav obuhvaćen istim sustavom upravljanja kvalitetom;

- (d) dokumentaciju o sustavu upravljanja kvalitetom koja obuhvaća sve aspekte navedene u članku 17.;
- (e) opis uspostavljenih postupaka kojima se osigurava da sustav upravljanja kvalitetom ostane adekvatan i djelotvoran;
- (f) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu.

3.2. Prijavljeno tijelo ocjenjuje sustav upravljanja kvalitetom i utvrđuje udovoljava li on zahtjevima iz članka 17.

O toj se odluci obavješćuje dobavljač ili njegov ovlašteni zastupnik.

Ta obavijest sadržava zaključke ocjenjivanja sustava upravljanja kvalitetom i obrazloženu odluku o ocjeni.

3.3. Dobavljač nastavlja primjenjivati i održavati odobreni sustav upravljanja kvalitetom tako da ostane adekvatan i učinkovit.

3.4. Dobavljač obavješćuje prijavljeno tijelo o svakoj planiranoj promjeni odobrenog sustava upravljanja kvalitetom ili popisa UI sustava koji su njime obuhvaćeni.

Prijavljeno tijelo pregledava predložene promjene i donosi odluku o tome ispunjava li izmijenjeni sustav upravljanja kvalitetom i dalje zahtjeve iz točke 3.2. ili je potrebno ponovno ocjenjivanje.

Prijavljeno tijelo obavješćuje dobavljača o svojoj odluci. Ta obavijest sadržava zaključke pregleda promjena i obrazloženu odluku o ocjeni.

4. Kontrola tehničke dokumentacije

4.1. Uz zahtjev iz točke 3. dobavljač podnosi prijavljenom tijelu koje je sâm odabrao zahtjev za ocjenjivanje tehničke dokumentacije UI sustava koji dobavljač namjerava staviti na tržište ili u upotrebu i koji je obuhvaćen sustavom upravljanja kvalitetom iz točke 3.

4.2. Taj zahtjev sadržava:

- (a) ime i adresu dobavljača;
- (b) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu;
- (c) tehničku dokumentaciju iz Priloga IV.

4.3. Prijavljeno tijelo pregledava tu tehničku dokumentaciju. Ako je to relevantno i ograničeno na ono što je potrebno za ispunjavanje njegovih zadaća, prijavljenom tijelu odobrava se puni pristup upotrijebljenim skupovima podataka za treniranje, validaciju i testiranje, među ostalim, prema potrebi i podložno sigurnosnim zaštitnim mjerama, putem aplikacijskih programskih sučelja ili drugih relevantnih tehničkih sredstava i alata koji omogućuju daljinski pristup.

- 4.4. Pri pregledu tehničke dokumentacije prijavljeno tijelo može zatražiti da dobavljač dostavi dodatne dokaze ili provede dodatna testiranja kako bi se omogućilo pravilno ocjenjivanje sukladnosti UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2.
- Ako prijavljeno tijelo nije zadovoljno testiranjima koja je proveo dobavljač, ono prema potrebi samo izravno provodi adekvatna testiranja.
- 4.5. Ako je to potrebno za ocjenjivanje sukladnosti visokorizičnog UI sustava sa zahtjevima utvrđenima u poglavlju III. odjeljku 2., nakon što su svi drugi razumni načini provjere sukladnosti iscrpljeni ili su se pokazali nedostatnima, i na obrazložen zahtjev, prijavljenom tijelu također se odobrava pristup modelima za treniranje i istreniranim modelima UI sustava, uključujući njegove relevantne parametre. Na taj pristup primjenjuje se postojeće pravo Unije u području zaštite intelektualnog vlasništva i poslovnih tajni.
- 4.6. O odluci prijavljenog tijela obavješćuje se dobavljač ili njegov ovlašteni zastupnik. Ta obavijest sadržava zaključke ocjenjivanja tehničke dokumentacije i obrazloženu odluku o ocjeni.

Ako je UI sustav sukladan sa zahtjevima iz poglavlja III. odjeljka 2., prijavljeno tijelo izdaje potvrdu Unije o ocjenjivanju tehničke dokumentacije. Ta potvrda sadržava ime i adresu dobavljača, zaključke pregleda, uvjete valjanosti potvrde (ako postoje) i podatke potrebne za identifikaciju dotičnog UI sustava.

Potvrda i njezini prilozi sadržavaju sve relevantne informacije potrebne za omogućivanje evaluacije sukladnosti UI sustava i, prema potrebi, za kontrolu UI sustava tijekom korištenja.

Ako UI sustav nije sukladan sa zahtjevima iz poglavlja III. odjeljka 2., prijavljeno tijelo odbija izdati potvrdu Unije o ocjenjivanju tehničke dokumentacije te o tome obavješćuje podnositelja zahtjeva, uz detaljno obrazloženje odbijanja.

Ako UI sustav ne ispunjava zahtjev u pogledu podataka upotrijebljenih za njegovo treniranje, prije podnošenja zahtjeva za novo ocjenjivanje sukladnosti bit će potrebno ponovno treniranje dotičnog UI sustava. U tom slučaju obrazložena odluka prijavljenog tijela o odbijanju izdavanja potvrde Unije o ocjenjivanju tehničke dokumentacije sadržava konkretne argumente o kvaliteti podataka upotrijebljenih za treniranje UI sustava, a posebno o razlozima za utvrđivanje neusklađenosti.

- 4.7. Svaku promjenu UI sustava koja bi mogla utjecati na usklađenost UI sustava sa zahtjevima ili na njegovu namjenu ocjenjuje prijavljeno tijelo koje je izdalo potvrdu Unije o ocjenjivanju tehničke dokumentacije. Dobavljač obavješćuje to prijavljeno tijelo o svojoj namjeri da uvede neku od navedenih promjena ili ako na neki drugi način sazna za pojavu takvih promjena. Prijavljeno tijelo ocjenjuje planirane promjene i odlučuje je li zbog njih potrebno novo ocjenjivanje sukladnosti u skladu s člankom 43. stavkom 4. ili se za njih može izdati dodatak potvrdi Unije o ocjenjivanju tehničke dokumentacije. U potonjem slučaju prijavljeno tijelo ocjenjuje promjene, obavješćuje dobavljača o svojoj odluci te, ako promjene odobri, dobavljaču izdaje dodatak potvrdi Unije o ocjenjivanju tehničke dokumentacije.

5. Nadzor nad odobrenim sustavom upravljanja kvalitetom
- 5.1. Svrha je nadzora koji provodi prijavljeno tijelo iz točke 3. osigurati da dobavljač ispunjava uvjete odobrenog sustava upravljanja kvalitetom.
- 5.2. Za potrebe ocjenjivanja dobavljač prijavljenom tijelu omogućuje pristup prostorima u kojima se odvijaju dizajniranje, razvoj i testiranje UI sustava. Osim toga, dobavljač prijavljenom tijelu daje sve potrebne informacije.
- 5.3. Prijavljeno tijelo provodi periodične revizije kako bi potvrdilo da dobavljač provodi i primjenjuje sustav upravljanja kvalitetom te dobavljaču dostavlja izvješće o reviziji. U okviru tih revizija prijavljeno tijelo može provesti dodatna testiranja UI sustava za koje je izdana potvrda Unije o ocjenjivanju tehničke dokumentacije.
-

PRILOG VIII.

Informacije koje se moraju dostaviti pri registraciji
visokorizičnih UI sustava u skladu s člankom 49.

Odjeljak A – Informacije koje moraju dostaviti dobavljači visokorizičnih UI sustava
u skladu s člankom 49. stavkom 1.

Za visokorizične UI sustave koji se moraju registrirati u skladu s člankom 49. stavkom 1.
dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. ime, adresa i kontaktni podaci dobavljača;
2. ako informacije dostavlja druga osoba u ime dobavljača, ime, adresa i kontaktni podaci te osobe;
3. ime, adresa i kontaktni podaci ovlaštenog zastupnika, ako je primjenjivo;
4. trgovačko ime UI sustava i sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;
5. opis namjene UI sustava te komponenti i funkcija koje podržava taj UI sustav;
6. osnovni i sažet opis informacija koje sustav upotrebljava (podaci, ulazne vrijednosti) i njegova logika funkcioniranja;

7. status UI sustava (stavljen na tržište ili u upotrebi; više nije stavljen na tržište / u upotrebi, opozvan);
8. vrsta, broj i datum isteka potvrde koju je izdalo prijavljeno tijelo te ime ili identifikacijski broj tog prijavljenog tijela, ako je primjenjivo;
9. skenirani primjerak potvrde iz točke 8., ako je primjenjivo;
10. imena država članica u kojima je UI sustav stavljen na tržište, u upotrebu ili na raspolaganje u Uniji;
11. primjerak EU izjave o sukladnosti iz članka 47.;
12. upute za korištenje u elektroničkom formatu; te se informacije ne dostavljaju za visokorizične UI sustave u području kaznenog progona ili migracija, azila i upravljanja nadzorom državne granice iz Priloga III. točaka 1., 6. i 7.;
13. URL adresa za dodatne informacije (nije obvezno).

Odjeljak B – Informacije koje moraju dostaviti dobavljači visokorizičnih UI sustava
u skladu s člankom 49. stavkom 2.

Za UI sustave koji se moraju registrirati u skladu s člankom 49. stavkom 2. dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. ime, adresa i kontaktni podaci dobavljača;
2. ako informacije dostavlja druga osoba u ime dobavljača, ime, adresa i kontaktni podaci te osobe;
3. ime, adresa i kontaktni podaci ovlaštenog zastupnika, ako je primjenjivo;
4. trgovačko ime UI sustava i sve dodatne nedvosmislene referentne oznake koje omogućuju identifikaciju i sljedivost UI sustava;
5. opis namjene UI sustava;
6. uvjet ili uvjeti iz članka 6. stavka 3. na temelju kojih se UI sustav ne smatra visokorizičnim;
7. kratak sažetak obrazloženja zašto se UI sustav ne smatra visokorizičnim pri primjeni postupka iz članka 6. stavka 3.;
8. status UI sustava (stavljen na tržište ili u upotrebi; više nije stavljen na tržište / u upotrebi, opozvan);
9. imena država članica u kojima je UI sustav stavljen na tržište, u upotrebu ili na raspolaganje u Uniji.

Odjeljak C – Informacije koje moraju dostaviti subjekti koji uvode visokorizične UI sustave
u skladu s člankom 49. stavkom 3.

Za visokorizične UI sustave koji se moraju registrirati u skladu s člankom 49. stavkom 3.
dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. ime, adresa i kontaktni podaci subjekta koji uvodi sustav;
2. ime, adresa i kontaktni podaci osobe koja dostavlja informacije u ime subjekta koji uvodi sustav;
3. URL adresa unosa UI sustava u bazu podataka EU-a od strane njegova dobavljača;
4. sažetak nalaza procjene učinka na temeljna prava provedene u skladu s člankom 27.;
5. sažetak procjene učinka na zaštitu podataka provedene u skladu s člankom 35. Uredbe (EU) 2016/679 ili člankom 27. Direktive (EU) 2016/680 kako je navedeno u članku 26. stavku 8. ove Uredbe, ako je primjenjivo.

PRILOG IX.

Informacije koje se moraju dostaviti pri registraciji visokorizičnih UI sustava iz priloga III.
u vezi s testiranjem u stvarnim uvjetima u skladu s člankom 60.

U vezi s testiranjem u stvarnim uvjetima koje se mora registrirati u skladu s člankom 60. dostavljaju se, a nakon toga ažuriraju, sljedeće informacije:

1. jedinstveni identifikacijski broj na razini Unije za testiranje u stvarnim uvjetima;
2. ime i kontaktni podaci dobavljača ili potencijalnog dobavljača i subjekata koji uvode sustav koji sudjeluju u testiranju u stvarnim uvjetima;
3. kratak opis UI sustava i njegove namjene te druge informacije potrebne za identifikaciju sustava;
4. sažetak glavnih karakteristika plana testiranja u stvarnim uvjetima;
5. informacije o suspenziji ili obustavi testiranja u stvarnim uvjetima.

PRILOG X.

Zakonodavni akti Unije o opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde

1. Schengenski informacijski sustav

- (a) Uredba (EU) 2018/1860 Europskog parlamenta i Vijeća od 28. studenoga 2018. o upotrebi Schengenskog informacijskog sustava za vraćanje državljana trećih zemalja s nezakonitim boravkom (SL L 312, 7.12.2018., str. 1.);
- (b) Uredba (EU) 2018/1861 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području granične kontrole i o izmjeni Konvencije o provedbi Schengenskog sporazuma te o izmjeni i stavljanju izvan snage Uredbe (EZ) br. 1987/2006 (SL L 312, 7.12.2018., str. 14.);
- (c) Uredba (EU) 2018/1862 Europskog parlamenta i Vijeća od 28. studenoga 2018. o uspostavi, radu i upotrebi Schengenskog informacijskog sustava (SIS) u području policijske suradnje i pravosudne suradnje u kaznenim stvarima, izmjeni i stavljanju izvan snage Odluke Vijeća 2007/533/PUP i stavljanju izvan snage Uredbe (EZ) br. 1986/2006 Europskog parlamenta i Vijeća i Odluke Komisije 2010/261/EU (SL L 312, 7.12.2018., str. 56.).

2. Vizni informacijski sustav

- (a) Uredba (EU) 2021/1133 Europskog parlamenta i Vijeća od 7. srpnja 2021. o izmjeni uredaba (EU) br. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 i (EU) 2019/818 u pogledu utvrđivanja uvjeta za pristup drugim informacijskim sustavima EU-a za potrebe viznog informacijskog sustava (SL L 248, 13.7.2021., str. 1.);
- (b) Uredba (EU) 2021/1134 Europskog parlamenta i Vijeća od 7. srpnja 2021. o izmjeni uredaba (EZ) br. 767/2008, (EZ) br. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 i (EU) 2019/1896 Europskog parlamenta i Vijeća te o stavljanju izvan snage odluka Vijeća 2004/512/EZ i 2008/633/PUP u svrhu reforme viznog informacijskog sustava (SL L 248, 13.7.2021., str. 11.).

3. Eurodac

Uredba (EU) 2024/... Europskog parlamenta i Vijeća o uspostavi sustava „Eurodac” za usporedbu biometrijskih podataka radi djelotvorne primjene uredaba (EU) 2024/... (EU) 2024/... Europskog parlamenta i Vijeća i Direktive Vijeća 2001/55/EZ te radi utvrđivanja identiteta državljanina treće zemlje i osoba bez državljanstva s nezakonitim boravkom i o zahtjevima tijela za izvršavanje zakonodavstva država članica i Europolu za usporedbu s podacima iz Eurodaca u svrhu izvršavanja zakonodavstva, o izmjeni uredaba (EU) 2018/1240 i (EU) 2019/818 Europskog parlamenta i Vijeća te o stavljanju izvan snage Uredbe (EU) br. 603/2013 Europskog parlamenta i Vijeća⁺.

4. Sustav ulaska/izlaska

Uredba (EU) 2017/2226 Europskog parlamenta i Vijeća od 30. studenoga 2017. o uspostavi sustava ulaska/izlaska (EES) za registraciju podataka o ulasku i izlasku te podataka o odbijanju ulaska za državljane trećih zemalja koji prelaze vanjske granice država članica i određivanju uvjeta za pristup EES-u za potrebe izvršavanja zakonodavstva te o izmjeni Konvencije o provedbi Schengenskog sporazuma i uredbi (EZ) br. 767/2008 i (EU) br. 1077/2011 (SL L 327, 9.12.2017., str. 20.).

⁺ SL: molimo unijeti u tekst broj uredbe iz dokumenta PE-CONS 15/24 (2016/0132(COD)), a u bilješku broj, datum, naslov i upućivanje na SL za tu uredbu.

5. Europski sustav za informacije o putovanjima i odobravanje putovanja
- (a) Uredba (EU) 2018/1240 Europskog parlamenta i Vijeća od 12. rujna 2018. o uspostavi europskog sustava za informacije o putovanjima i odobravanje putovanja (ETIAS) i izmjeni uredaba (EU) br. 1077/2011, (EU) br. 515/2014, (EU) 2016/399, (EU) 2016/1624 i (EU) 2017/2226 (SL L 236, 19.9.2018., str. 1.);
- (b) Uredba (EU) 2018/1241 Europskog parlamenta i Vijeća od 12. rujna 2018. o izmjeni Uredbe (EU) 2016/794 u svrhu uspostave europskog sustava za informacije o putovanjima i odobravanje putovanja (ETIAS) (SL L 236, 19.9.2018., str. 72.).
6. Europski informacijski sustav kaznene evidencije za državljane trećih zemalja i osobe bez državljanstva
- Uredba (EU) 2019/816 Europskog parlamenta i Vijeća od 17. travnja 2019. o uspostavi centraliziranog sustava za utvrđivanje država članica koje imaju podatke o osuđujućim presudama protiv državljana trećih zemalja i osoba bez državljanstva (sustav ECRIS-TCN) za dopunu Europskog informacijskog sustava kaznene evidencije te o izmjeni Uredbe (EU) 2018/1726 (SL L 135, 22.5.2019., str. 1.).

7. Interoperabilnost

- (a) Uredba (EU) 2019/817 Europskog parlamenta i Vijeća od 20. svibnja 2019. o uspostavi okvira za interoperabilnost informacijskih sustava EU-a u području granica i viza i izmjeni uredaba (EZ) br. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 i (EU) 2018/1861 Europskog parlamenta i Vijeća te odluka Vijeća 2004/512/EZ i 2008/633/PUP (SL L 135, 22.5.2019., str. 27.);
 - (b) Uredba (EU) 2019/818 Europskog parlamenta i Vijeća od 20. svibnja 2019. o uspostavi okvira za interoperabilnost informacijskih sustava EU-a u području policijske i pravosudne suradnje, azila i migracija i izmjeni uredaba (EU) 2018/1726, (EU) 2018/1862 i (EU) 2019/816 (SL L 135, 22.5.2019., str. 85.).
-

PRILOG XI.

Tehnička dokumentacija iz članka 53. stavka 1. točke (a) – tehnička dokumentacija
za dobavljače UI modela opće namjene

Odjeljak 1.

Informacije koje moraju dostaviti svi dobavljači UI modelâ opće namjene

Tehnička dokumentacija iz članka 53. stavka 1. sadržava barem sljedeće informacije, ovisno o
veličini i profilu rizika modela:

1. Opći opis UI modela opće namjene, uključujući:
 - (a) zadaće koje bi model trebao obavljati te vrstu i prirodu UI sustava u koje se može integrirati;
 - (b) primjenjive politike u pogledu prihvatljivog korištenja;
 - (c) datum stavljanja na tržište i metode distribucije;
 - d) arhitekturu i broj parametara;
 - (e) modalitet (npr. tekst, slika) i format ulaznih i izlaznih podataka;
 - (f) licenciju.

2. Detaljan opis elemenata modela iz točke 1. i relevantne informacije o postupku njegova razvoja, uključujući sljedeće elemente:
- (a) tehnička sredstva (npr. upute za korištenje, infrastruktura, alati) potrebna za integraciju UI modela opće namjene u UI sustave;
 - (b) specifikacije dizajna modela i postupka treniranja, uključujući metodologije i tehnike treniranja, najvažnije odabire u pogledu dizajna, uključujući obrazloženja i pretpostavke; informacije o tome što bi model svojim dizajnom trebao optimizirati i relevantnost različitih parametara, ako je primjenjivo;
 - (c) informacije o podacima upotrijebljenima za treniranje, testiranje i validaciju, ako je primjenjivo, uključujući vrstu i podrijetlo podataka i metodologije skrbi o podacima (npr. čišćenje, filtriranje itd.), količinu podataka, njihov opseg i glavne karakteristike; način na koji su podaci dobiveni i odabrani, kao i sve druge mjere za otkrivanje neprimjerenosti izvora podataka i metode za otkrivanje utvrdivih pristranosti, ako je primjenjivo;
 - (d) računalne resurse upotrijebljene za treniranje modela (npr. broj matematičkih operacija nad s brojevima s pomičnim zarezom), vrijeme treniranja i druge relevantne pojedinosti povezane s treniranjem;
 - (e) poznatu ili procijenjenu potrošnju energije modela.

Kad je riječ o točki (e), ako je potrošnja energije modela nepoznata, potrošnja energije može se temeljiti na informacijama o upotrijebljenim računalnim resursima.

Odjeljak 2.

Dodatne informacije koje moraju dostaviti
dobavljači UI modela opće namjene sa sistemskim rizikom

1. Detaljan opis strategija evaluacije, uključujući rezultate evaluacije, na temelju dostupnih javnih evaluacijskih protokola i alata ili drugih metodologija evaluacije. Strategije evaluacije uključuju evaluacijske kriterije, parametre i metodologiju za utvrđivanje ograničenja.
 2. Ako je primjenjivo, detaljan opis mjera uspostavljenih u svrhu provedbe unutarnjeg i/ili vanjskog neprijateljskog testiranja (npr. penetracijsko testiranje) i prilagodaba modela, uključujući usklađivanje i doradu.
 3. Ako je primjenjivo, detaljan opis arhitekture sustava koji objašnjava kako se softverske komponente međusobno nadopunjuju ili potpomažu te kako su integrirane u cjelokupnu obradu.
-

PRILOG XII.

Informacije o transparentnosti iz članka 53. stavka 1. točke (b)

– tehnička dokumentacija koju dobavljači UI modela opće namjene stavljaju na raspolaganje dobavljačima niže u lancu koji integriraju model u svoj UI sustav

Informacije iz članka 53. stavka 1. točke (b) sadržavaju barem sljedeće elemente:

1. opći opis UI modela opće namjene, uključujući:
 - (a) zadaće koje bi model trebao obavljati te vrstu i prirodu UI sustava u koje se može integrirati;
 - (b) primjenjive politike u pogledu prihvatljivog korištenja;
 - (c) datum stavljanja na tržište i metode distribucije;
 - (d) način na koji je model u interakciji s hardverom ili softverom koji nije dio samog modela ili na koji se može upotrijebiti za takvu interakciju, ako je primjenjivo;
 - (e) verzije relevantnog softvera povezanog s korištenjem UI modela opće namjene, ako je primjenjivo;
 - (f) arhitekturu i broj parametara;
 - (g) modalitet (npr. tekst, slika) i format ulaznih i izlaznih podataka;
 - (h) licenciju za model;

2. opis elemenata UI modela i postupka njegova razvoja, uključujući:
- (a) tehnička sredstva (npr. upute za korištenje, infrastruktura, alati) potrebna za integraciju UI modela opće namjene u UI sustave;
 - (b) modalitet (npr. tekst, slika itd.) i format ulaznih i izlaznih podataka te njihova maksimalna veličina (npr. veličina kontekstualnog prozora itd.);
 - (c) informacije o podacima upotrijebljenima za treniranje, testiranje i validaciju, ako je primjenjivo, uključujući vrstu i podrijetlo podataka i metodologije skrbi o podacima.
-

PRILOG XIII.

Kriteriji za određivanje UI modela opće namjene
sa sistemskim rizikom iz članka 51.

Kako bi utvrdila ima li određeni UI model opće namjene sposobnosti ili učinak jednakovrijedne onima iz članka 51. stavka 1. točke (a), Komisija uzima u obzir sljedeće kriterije:

- (a) broj parametara modela;
- (b) kvalitetu ili veličinu skupa podataka, primjerice mjereno tokenima;
- (c) količinu računanja upotrijebljenu za treniranje modela, izmjerenu u matematičkim operacijama nad brojevima s pomičnim zarezom ili izraženu kombinacijom drugih varijabli kao što su procijenjeni troškovi treniranja, procijenjeno vrijeme potrebno za treniranje ili procijenjena potrošnja energije za treniranje;
- (d) ulazne i izlazne modalitete modela, kao što su pretvaranje teksta u tekst (veliki jezični modeli), pretvaranje teksta u sliku, multimodalnost i najnoviji pragovi za utvrđivanje sposobnosti visokog učinka za svaki modalitet, kao i specifičnu vrstu ulaznih i izlaznih podataka (npr. biološke sekvence);
- (e) referentne vrijednosti i evaluacije sposobnosti modela, što uključuje uzimanje u obzir broja zadataka bez dodatnog treniranja, prilagodljivost za učenje novih, različitih zadataka, njegovu razinu autonomije i skalabilnosti, alate kojima ima pristup;

- (f) ima li model zbog svojeg dosega znatan utjecaj na unutarnje tržište, što se pretpostavlja ako je stavljen na raspolaganje najmanje 10 000 registriranih poslovnih korisnika s poslovnim nastanom u Uniji;
 - (g) broj registriranih krajnjih korisnika.”.
-

RETTIFICA

del regolamento (UE) del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale)

(PE-CONS 24/1/24 REV 1, 14 giugno 2024)

Il regolamento contenuto nel documento PE-CONS 24/1/24 REV 1 va letto come segue:

REGOLAMENTO (UE) 2024/...
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 13 giugno 2024

**che stabilisce regole armonizzate sull'intelligenza artificiale
e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013,
(UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144
e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828
(regolamento sull'intelligenza artificiale)**

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare gli articoli 16 e 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo¹¹⁷,

visto il parere della Banca centrale europea¹¹⁸,

visto il parere del Comitato delle regioni¹¹⁹,

deliberando secondo la procedura legislativa ordinaria¹²⁰,

¹¹⁷ GU C 517 del 22.12.2021, pag. 56.

¹¹⁸ GU C 115 dell'11.3.2022, pag. 5.

¹¹⁹ GU C 97 del 28.2.2022, pag. 60.

¹²⁰ Posizione del Parlamento europeo del 13 marzo 2024 (non ancora pubblicata sulla Gazzetta ufficiale) e decisione del Consiglio del 21 maggio 2024.

considerando quanto segue:

- (1) Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea (“Carta”), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione. Il presente regolamento garantisce la libera circolazione transfrontaliera di beni e servizi basati sull'IA, impedendo così agli Stati membri di imporre restrizioni allo sviluppo, alla commercializzazione e all'uso di sistemi di IA, salvo espressa autorizzazione del presente regolamento.
- (2) Il presente regolamento dovrebbe essere applicato conformemente ai valori dell'Unione sanciti dalla Carta agevolando la protezione delle persone fisiche, delle imprese, della democrazia e dello Stato di diritto e la protezione dell'ambiente, promuovendo nel contempo l'innovazione e l'occupazione e rendendo l'Unione un leader nell'adozione di un'IA affidabile.

- (3) I sistemi di IA possono essere facilmente impiegati in un'ampia gamma di settori dell'economia e in molte parti della società, anche a livello transfrontaliero, e possono facilmente circolare in tutta l'Unione. Alcuni Stati membri hanno già preso in esame l'adozione di regole nazionali per garantire che l'IA sia affidabile e sicura e sia sviluppata e utilizzata nel rispetto degli obblighi in materia di diritti fondamentali. Normative nazionali divergenti possono determinare una frammentazione del mercato interno e diminuire la certezza del diritto per gli operatori che sviluppano, importano o utilizzano sistemi di IA. È pertanto opportuno garantire un livello di protezione costante ed elevato in tutta l'Unione al fine di conseguire un'IA affidabile, mentre dovrebbero essere evitate le divergenze che ostacolano la libera circolazione, l'innovazione, la diffusione e l'adozione dei sistemi di IA e dei relativi prodotti e servizi nel mercato interno, stabilendo obblighi uniformi per gli operatori e garantendo la tutela uniforme dei motivi imperativi di interesse pubblico e dei diritti delle persone in tutto il mercato interno, sulla base dell'articolo 114 del trattato sul funzionamento dell'Unione europea (TFUE). Nella misura in cui il presente regolamento prevede regole specifiche sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, consistenti in limitazioni dell'uso dei sistemi di IA per l'identificazione biometrica remota a fini di attività di contrasto, dell'uso dei sistemi di IA per la valutazione dei rischi delle persone fisiche a fini di attività di contrasto e dell'uso dei sistemi di IA di categorizzazione biometrica a fini di attività di contrasto, è opportuno basare il presente regolamento, per quanto riguarda tali regole specifiche, sull'articolo 16 TFUE. Alla luce di tali regole specifiche e del ricorso all'articolo 16 TFUE, è opportuno consultare il comitato europeo per la protezione dei dati.

- (4) L'IA consiste in una famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'IA, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi.
- (5) L'IA può nel contempo, a seconda delle circostanze relative alla sua applicazione, al suo utilizzo e al suo livello di sviluppo tecnologico specifici, comportare rischi e pregiudicare gli interessi pubblici e i diritti fondamentali tutelati dal diritto dell'Unione. Tale pregiudizio può essere sia materiale sia immateriale, compreso il pregiudizio fisico, psicologico, sociale o economico.

- (6) In considerazione dell'impatto significativo che l'IA può avere sulla società e della necessità di creare maggiore fiducia, è essenziale che l'IA e il suo quadro normativo siano sviluppati conformemente ai valori dell'Unione sanciti dall'articolo 2 del trattato sull'Unione europea (TUE), ai diritti e alle libertà fondamentali sanciti dai trattati e, conformemente all'articolo 6 TUE, alla Carta. Come prerequisito, l'IA dovrebbe essere una tecnologia antropocentrica. Dovrebbe fungere da strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani.
- (7) Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire regole comuni per i sistemi di IA ad alto rischio. Tali regole dovrebbero essere coerenti con la Carta, non discriminatorie e in linea con gli impegni commerciali internazionali dell'Unione. Dovrebbero inoltre tenere conto della dichiarazione europea sui diritti e i principi digitali per il decennio digitale e degli orientamenti etici per un'IA affidabile del gruppo di esperti ad alto livello sull'intelligenza artificiale (AI HLEG).

- (8) Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione dell'IA nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, come riconosciuti e tutelati dal diritto dell'Unione. Per conseguire tale obiettivo, è opportuno stabilire regole che disciplinino l'immissione sul mercato, la messa in servizio e l'uso di determinati sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e consentendo a tali sistemi di beneficiare del principio della libera circolazione di beni e servizi. Tali norme dovrebbero essere chiare e solide nel tutelare i diritti fondamentali, sostenere nuove soluzioni innovative e consentire un ecosistema europeo di attori pubblici e privati che creino sistemi di IA in linea con i valori dell'Unione e sblocchino il potenziale della trasformazione digitale in tutte le regioni dell'Unione. Stabilendo tali regole nonché le misure a sostegno dell'innovazione, con particolare attenzione alle piccole e medie imprese (PMI), comprese le start-up, il presente regolamento contribuisce all'obiettivo di promuovere l'approccio antropocentrico europeo all'IA ed essere un leader mondiale nello sviluppo di un'IA sicura, affidabile ed etica, come affermato dal Consiglio europeo¹²¹, e garantisce la tutela dei principi etici, come specificamente richiesto dal Parlamento europeo¹²².

¹²¹ Consiglio europeo, riunione straordinaria del Consiglio europeo (1 e 2 ottobre 2020) – Conclusioni, EUCO 13/20, 2020, pag. 6.

¹²² Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)).

- (9) È opportuno che le norme armonizzate applicabili all'immissione sul mercato, alla messa in servizio e all'uso di sistemi di IA ad alto rischio siano stabilite conformemente al regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio¹²³, alla decisione n. 768/2008/CE del Parlamento europeo e del Consiglio¹²⁴ e al regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio¹²⁵ ("nuovo quadro legislativo"). Le norme armonizzate stabilite nel presente regolamento dovrebbero applicarsi in tutti i settori e, in linea con il nuovo quadro legislativo, non dovrebbero pregiudicare il vigente diritto dell'Unione, in particolare in materia di protezione dei dati, tutela dei consumatori, diritti fondamentali, occupazione e protezione dei lavoratori e sicurezza dei prodotti, al quale il presente regolamento è complementare. Di conseguenza, restano impregiudicati e pienamente applicabili tutti i diritti e i mezzi di ricorso previsti da tali disposizioni di diritto dell'Unione a favore dei consumatori e delle altre persone su cui i sistemi di IA possono avere un impatto negativo, anche in relazione al risarcimento di eventuali danni a norma della direttiva 85/374/CEE del Consiglio¹²⁶.

¹²³ Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

¹²⁴ Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

¹²⁵ Regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti e che modifica la direttiva 2004/42/CE e i regolamenti (CE) n. 765/2008 e (UE) n. 305/2011 (GU L 169 del 25.6.2019, pag. 1).

¹²⁶ Direttiva 85/374/CEE del Consiglio, del 25 luglio 1985, relativa al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri in materia di responsabilità per danno da prodotti difettosi (GU L 210 del 7.8.1985, pag. 29).

Inoltre, nel contesto dell'occupazione e della protezione dei lavoratori, il presente regolamento non dovrebbe pertanto incidere sul diritto dell'Unione in materia di politica sociale né sul diritto del lavoro nazionale, in conformità del diritto dell'Unione, per quanto riguarda le condizioni di impiego e le condizioni di lavoro, comprese la salute e la sicurezza sul luogo di lavoro, e il rapporto tra datori di lavoro e lavoratori. Il presente regolamento non dovrebbe inoltre pregiudicare l'esercizio dei diritti fondamentali riconosciuti dagli Stati membri e a livello di Unione, compresi il diritto o la libertà di sciopero o il diritto o la libertà di intraprendere altre azioni contemplate dalla disciplina delle relazioni industriali negli Stati membri nonché il diritto di negoziare, concludere ed eseguire accordi collettivi, o di intraprendere azioni collettive in conformità del diritto nazionale. Il presente regolamento dovrebbe lasciare impregiudicate le disposizioni volte a migliorare le condizioni di lavoro nel lavoro mediante piattaforme digitali di cui alla direttiva del Parlamento europeo e del Consiglio relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali. Inoltre, il presente regolamento mira a rafforzare l'efficacia di tali diritti e mezzi di ricorso esistenti definendo requisiti e obblighi specifici, anche per quanto riguarda la trasparenza, la documentazione tecnica e la conservazione delle registrazioni dei sistemi di IA. Oltre a ciò, gli obblighi imposti a vari operatori coinvolti nella catena del valore dell'IA a norma del presente regolamento dovrebbero applicarsi senza pregiudizio del diritto nazionale, in conformità del diritto dell'Unione, e avere l'effetto di limitare l'uso di determinati sistemi di IA qualora tale diritto non rientri nell'ambito di applicazione del presente regolamento o persegua obiettivi legittimi di interesse pubblico diversi da quelli perseguiti dal presente regolamento. Ad esempio, il presente regolamento non dovrebbe incidere sulla normativa nazionale in materia di lavoro e sulla normativa in materia di protezione dei minori, ossia le persone di età inferiore ai 18 anni, tenendo conto del commento generale n. 25 della Convenzione sui diritti dell'infanzia e dell'adolescenza (2021) sui diritti dei minori in relazione all'ambiente digitale, nella misura in cui esse non riguardino in modo specifico i sistemi di IA e perseguano altri obiettivi legittimi di interesse pubblico.

- (10) Il diritto fondamentale alla protezione dei dati personali è garantito in particolare dai regolamenti (UE) 2016/679¹²⁷ e (UE) 2018/1725¹²⁸ del Parlamento europeo e del Consiglio e dalla direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio¹²⁹. La direttiva 2002/58/CE del Parlamento europeo e del Consiglio¹³⁰ tutela inoltre la vita privata e la riservatezza delle comunicazioni, in particolare stabilendo le condizioni per l'archiviazione di dati personali e non personali e l'accesso ai dati in apparecchi terminali. Tali atti giuridici dell'Unione costituiscono la base per un trattamento sostenibile e responsabile dei dati, anche nei casi in cui gli insiemi di dati comprendono una combinazione di dati personali e non personali. Il presente regolamento non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti.

¹²⁷ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

¹²⁸ Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

¹²⁹ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

¹³⁰ Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

Inoltre, lascia impregiudicati gli obblighi dei fornitori e dei deployer dei sistemi di IA nel loro ruolo di titolari del trattamento o responsabili del trattamento derivanti dal diritto dell'Unione o nazionale in materia di protezione dei dati personali, nella misura in cui la progettazione, lo sviluppo o l'uso di sistemi di IA comportino il trattamento di dati personali. È inoltre opportuno chiarire che gli interessati continuano a godere di tutti i diritti e le garanzie loro conferiti da tale diritto dell'Unione, compresi i diritti connessi al processo decisionale esclusivamente automatizzato relativo alle persone fisiche, compresa la profilazione. Norme armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA istituiti a norma del presente regolamento dovrebbero facilitare l'efficace attuazione e consentire l'esercizio dei diritti degli interessati e di altri mezzi di ricorso garantiti dal diritto dell'Unione in materia di protezione dei dati personali nonché degli altri diritti fondamentali.

- (11) Il presente regolamento non dovrebbe pregiudicare le disposizioni relative alla responsabilità dei prestatori intermediari di cui al regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio¹³¹.

¹³¹ Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU L 277 del 27.10.2022, pag. 1).

- (12) La nozione di "sistema di IA" di cui al presente regolamento dovrebbe essere definita in maniera chiara e dovrebbe essere strettamente allineata al lavoro delle organizzazioni internazionali che si occupano di IA al fine di garantire la certezza del diritto, agevolare la convergenza internazionale e un'ampia accettazione, prevedendo nel contempo la flessibilità necessaria per agevolare i rapidi sviluppi tecnologici in questo ambito. Inoltre, la definizione dovrebbe essere basata sulle principali caratteristiche dei sistemi di IA, che la distinguono dai tradizionali sistemi software o dagli approcci di programmazione più semplici, e non dovrebbe riguardare i sistemi basati sulle regole definite unicamente da persone fisiche per eseguire operazioni in modo automatico. Una caratteristica fondamentale dei sistemi di IA è la loro capacità inferenziale. Tale capacità inferenziale si riferisce al processo di ottenimento degli output, quali previsioni, contenuti, raccomandazioni o decisioni, che possono influenzare gli ambienti fisici e virtuali e alla capacità dei sistemi di IA di ricavare modelli o algoritmi, o entrambi, da input o dati. Le tecniche che consentono l'inferenza nella costruzione di un sistema di IA comprendono approcci di apprendimento automatico che imparano dai dati come conseguire determinati obiettivi e approcci basati sulla logica e sulla conoscenza che traggono inferenze dalla conoscenza codificata o dalla rappresentazione simbolica del compito da risolvere. La capacità inferenziale di un sistema di IA trascende l'elaborazione di base dei dati consentendo l'apprendimento, il ragionamento o la modellizzazione. Il termine "automatizzato" si riferisce al fatto che il funzionamento dei sistemi di IA prevede l'uso di macchine.

Il riferimento a obiettivi espliciti o impliciti sottolinea che i sistemi di IA possono operare in base a obiettivi espliciti definiti o a obiettivi impliciti. Gli obiettivi del sistema di IA possono essere diversi dalla finalità prevista del sistema di IA in un contesto specifico. Ai fini del presente regolamento, gli ambienti dovrebbero essere intesi come i contesti in cui operano i sistemi di IA, mentre gli output generati dal sistema di IA riflettono le diverse funzioni svolte dai sistemi di IA e comprendono previsioni, contenuti, raccomandazioni o decisioni. I sistemi di IA sono progettati per funzionare con livelli di autonomia variabili, il che significa che dispongono di un certo grado di autonomia di azione rispetto al coinvolgimento umano e di capacità di funzionare senza l'intervento umano. L'adattabilità che un sistema di IA potrebbe presentare dopo la diffusione si riferisce alle capacità di autoapprendimento, che consentono al sistema di cambiare durante l'uso. I sistemi di IA possono essere utilizzati come elementi indipendenti (stand-alone) o come componenti di un prodotto, a prescindere dal fatto che il sistema sia fisicamente incorporato nel prodotto (integrato) o assista la funzionalità del prodotto senza esservi incorporato (non integrato).

- (13) La nozione di "deployer" di cui al presente regolamento dovrebbe essere interpretata come qualsiasi persona fisica o giuridica, compresi un'autorità pubblica, un'agenzia o altro organismo, che utilizza un sistema di IA sotto la sua autorità, salvo nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale. A seconda del tipo di sistema di IA, l'uso del sistema può interessare persone diverse dal deployer.
- (14) La nozione di "dati biometrici" utilizzata nel presente regolamento dovrebbe essere interpretata alla luce della nozione di dati biometrici di cui all'articolo 4, punto 14, del regolamento (UE) 2016/679, all'articolo 3, punto 18, del regolamento (UE) 2018/172 e all'articolo 3, punto 13, della direttiva (UE) 2016/680. I dati biometrici possono consentire l'autenticazione, l'identificazione o la categorizzazione delle persone fisiche e il riconoscimento delle emozioni delle persone fisiche.
- (15) La nozione di "identificazione biometrica" di cui al presente regolamento dovrebbe essere definita come il riconoscimento automatico di caratteristiche fisiche, fisiologiche e comportamentali di una persona, quali il volto, il movimento degli occhi, la forma del corpo, la voce, la prosodia, l'andatura, la postura, la frequenza cardiaca, la pressione sanguigna, l'odore, la pressione esercitata sui tasti, allo scopo di determinare l'identità di una persona confrontando i suoi dati biometrici con quelli di altri individui memorizzati in una banca dati di riferimento, indipendentemente dal fatto che la persona abbia fornito il proprio consenso. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali.

- (16) La nozione di "categorizzazione biometrica" di cui al presente regolamento dovrebbe essere definita come l'assegnazione di persone fisiche a categorie specifiche sulla base dei loro dati biometrici. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti comportamentali o di personalità, la lingua, la religione, l'appartenenza a una minoranza nazionale, l'orientamento sessuale o politico. Ciò non comprende i sistemi di categorizzazione biometrica che sono una caratteristica puramente accessoria intrinsecamente legata a un altro servizio commerciale, il che significa che l'elemento non può, per ragioni tecniche oggettive, essere utilizzato senza il servizio principale e che l'integrazione di tale caratteristica o funzionalità non rappresenta un mezzo per eludere l'applicabilità delle norme del presente regolamento. Ad esempio, i filtri che classificano le caratteristiche facciali o del corpo utilizzate sui mercati online potrebbero costituire una tale caratteristica accessoria, in quanto possono essere utilizzati solo in relazione al servizio principale che consiste nel vendere un prodotto consentendo al consumatore di visualizzare in anteprima il prodotto su se stesso e aiutarlo a prendere una decisione di acquisto. Anche i filtri utilizzati nei servizi di social network online che classificano le caratteristiche facciali o del corpo per consentire agli utenti di aggiungere o modificare immagini o video potrebbero essere considerati una caratteristica accessoria, in quanto tale filtro non può essere utilizzato senza il servizio principale dei servizi di social network consistente nella condivisione di contenuti online.

- (17) È opportuno definire a livello funzionale la nozione di "sistema di identificazione biometrica remota" di cui al presente regolamento, quale sistema di IA destinato all'identificazione, tipicamente a distanza, di persone fisiche senza il loro coinvolgimento attivo mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento, a prescindere dalla tecnologia, dai processi o dai tipi specifici di dati biometrici utilizzati. Tali sistemi di identificazione biometrica remota sono generalmente utilizzati per percepire più persone o il loro comportamento simultaneamente al fine di facilitare in modo significativo l'identificazione di persone fisiche senza il loro coinvolgimento attivo. Sono esclusi i sistemi di IA destinati a essere utilizzati per la verifica biometrica, che include l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso di sicurezza a locali. Tale esclusione è giustificata dal fatto che detti sistemi hanno probabilmente un impatto minore sui diritti fondamentali delle persone fisiche rispetto ai sistemi di identificazione biometrica remota, che possono essere utilizzati per il trattamento dei dati biometrici di un numero elevato di persone senza il loro coinvolgimento attivo. Nel caso dei sistemi "in tempo reale", il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono tutti istantaneamente, quasi istantaneamente o in ogni caso senza ritardi significativi. A tale riguardo è opportuno impedire l'elusione delle regole del presente regolamento per quanto attiene all'uso "in tempo reale" dei sistemi di IA interessati prevedendo ritardi minimi. I sistemi "in tempo reale" comportano l'uso di materiale "dal vivo" o "quasi dal vivo" (ad esempio filmati) generato da una telecamera o da un altro dispositivo con funzionalità analoghe. Nel caso dei sistemi di identificazione a posteriori, invece, i dati biometrici sono già stati rilevati e il confronto e l'identificazione avvengono solo con un ritardo significativo. Si tratta di materiale, come immagini o filmati generati da telecamere a circuito chiuso o da dispositivi privati, che è stato generato prima che il sistema fosse usato in relazione alle persone fisiche interessate.

- (18) La nozione di "sistema di riconoscimento delle emozioni" di cui al presente regolamento dovrebbe essere definita come un sistema di IA finalizzato a identificare o inferire emozioni o intenzioni di persone fisiche, sulla base dei loro dati biometrici. La nozione si riferisce a emozioni o intenzioni quali felicità, tristezza, rabbia, sorpresa, disgusto, imbarazzo, eccitazione, vergogna, disprezzo, soddisfazione e divertimento. Non comprende stati fisici, quali dolore o affaticamento, compresi, ad esempio, ai sistemi utilizzati per rilevare lo stato di affaticamento dei piloti o dei conducenti professionisti al fine di prevenire gli incidenti. Non comprende neppure la semplice individuazione di espressioni, gesti o movimenti immediatamente evidenti, a meno che non siano utilizzati per identificare o inferire emozioni. Tali espressioni possono essere espressioni facciali di base quali un aggrottamento delle sopracciglia o un sorriso, gesti quali il movimento di mani, braccia o testa, o caratteristiche della voce di una persona, ad esempio una voce alta o un sussurro.

- (19) Ai fini del presente regolamento la nozione di "spazio accessibile al pubblico" dovrebbe essere intesa come riferita a qualsiasi luogo fisico accessibile a un numero indeterminato di persone fisiche e a prescindere dal fatto che il luogo in questione sia di proprietà pubblica o privata, indipendentemente dall'attività per la quale il luogo può essere utilizzato, quali il commercio (ad esempio negozi, ristoranti, bar), i servizi (ad esempio banche, attività professionali, ospitalità), lo sport (ad esempio piscine, palestre, stadi), i trasporti (ad esempio stazioni di autobus, metropolitane e ferroviarie, aeroporti, mezzi di trasporto), l'intrattenimento (ad esempio cinema, teatri, musei, sale da concerto e sale conferenze), il tempo libero o altro (ad esempio strade e piazze pubbliche, parchi, foreste, parchi giochi). Un luogo dovrebbe essere classificato come accessibile al pubblico anche se, indipendentemente da potenziali restrizioni di capacità o di sicurezza, l'accesso è soggetto a determinate condizioni predeterminate, che possono essere soddisfatte da un numero indeterminato di persone, quali l'acquisto di un biglietto o titolo di trasporto, la registrazione previa o il raggiungimento di una determinata età. Per contro, un luogo non dovrebbe essere considerato accessibile al pubblico se l'accesso è limitato a persone fisiche specifiche e definite attraverso il diritto dell'Unione o nazionale direttamente connesso alla pubblica sicurezza o attraverso la chiara manifestazione di volontà da parte della persona che ha l'autorità pertinente sul luogo. La sola possibilità concreta di accesso (ad esempio una porta sbloccata, un cancello aperto in una recinzione) non implica che il luogo sia accessibile al pubblico in presenza di indicazioni o circostanze che suggeriscono il contrario (ad esempio segnaletica che vieta o limita l'accesso). I locali delle imprese e delle fabbriche, come pure gli uffici e i luoghi di lavoro destinati ad essere accessibili solo dai pertinenti dipendenti e prestatori di servizi, sono luoghi non accessibili al pubblico. Gli spazi accessibili al pubblico non dovrebbero includere le carceri o i controlli di frontiera. Alcune altre zone possono comprendere sia aree non accessibili al pubblico che aree accessibili al pubblico, come l'atrio di un edificio residenziale privato da cui è possibile accedere a uno studio medico o un aeroporto. Non sono del pari contemplati gli spazi online, dato che non sono luoghi fisici. L'accessibilità di un determinato spazio al pubblico dovrebbe tuttavia essere determinata caso per caso, tenendo conto delle specificità della singola situazione presa in esame.

- (20) Al fine di ottenere i massimi benefici dai sistemi di IA proteggendo nel contempo i diritti fondamentali, la salute e la sicurezza e di consentire il controllo democratico, l'alfabetizzazione in materia di IA dovrebbe dotare i fornitori, i deployer e le persone interessate delle nozioni necessarie per prendere decisioni informate in merito ai sistemi di IA. Tali nozioni possono variare in relazione al contesto pertinente e possono includere la comprensione della corretta applicazione degli elementi tecnici durante la fase di sviluppo del sistema di IA, le misure da applicare durante il suo utilizzo, le modalità adeguate per interpretare l'output del sistema di IA e, nel caso delle persone interessate, le conoscenze necessarie per comprendere in che modo le decisioni adottate con l'assistenza dell'IA incideranno su di esse. Nel contesto dell'applicazione del presente regolamento, l'alfabetizzazione in materia di IA dovrebbe fornire a tutti i pertinenti attori della catena del valore dell'IA le conoscenze necessarie per garantire l'adeguata conformità e la sua corretta esecuzione. Inoltre, l'ampia attuazione delle misure di alfabetizzazione in materia di IA e l'introduzione di adeguate azioni di follow-up potrebbero contribuire a migliorare le condizioni di lavoro e, in ultima analisi, sostenere il consolidamento e il percorso di innovazione di un'IA affidabile nell'Unione. Il consiglio europeo per l'intelligenza artificiale ("consiglio per l'IA") dovrebbe sostenere la Commissione al fine di promuovere gli strumenti di alfabetizzazione in materia di IA, la sensibilizzazione del pubblico e la comprensione dei benefici, dei rischi, delle garanzie, dei diritti e degli obblighi in relazione all'uso dei sistemi di IA. In cooperazione con i pertinenti portatori di interessi, la Commissione e gli Stati membri dovrebbero agevolare l'elaborazione di codici di condotta volontari per migliorare l'alfabetizzazione in materia di IA tra le persone che si occupano di sviluppo, funzionamento e uso dell'IA.

- (21) Al fine di garantire condizioni di parità e una protezione efficace dei diritti e delle libertà delle persone in tutta l'Unione, è opportuno che le regole stabilite dal presente regolamento si applichino ai fornitori di sistemi di IA in modo non discriminatorio, a prescindere dal fatto che siano stabiliti nell'Unione o in un paese terzo, e ai deployer dei sistemi di IA stabiliti nell'Unione.
- (22) Alla luce della loro natura di sistemi digitali, è opportuno che determinati sistemi di IA rientrino nell'ambito di applicazione del presente regolamento anche quando non sono immessi sul mercato, né messi in servizio, né utilizzati nell'Unione. È il caso, ad esempio, di un operatore stabilito nell'Unione che appalta alcuni servizi a un operatore stabilito in un paese terzo in relazione a un'attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio. In tali circostanze il sistema di IA utilizzato dall'operatore in un paese terzo potrebbe trattare dati raccolti nell'Unione e da lì trasferiti nel rispetto della legge, e fornire all'operatore appaltante nell'Unione l'output di tale sistema di IA risultante da tale trattamento, senza che tale sistema di IA sia immesso sul mercato, messo in servizio o utilizzato nell'Unione. Al fine di impedire l'elusione del presente regolamento e di garantire una protezione efficace delle persone fisiche che si trovano nell'Unione, è opportuno che il presente regolamento si applichi anche ai fornitori e ai deployer di sistemi di IA stabiliti in un paese terzo, nella misura in cui l'output prodotto da tali sistemi è destinato a essere utilizzato nell'Unione.

Cionondimeno, per tener conto degli accordi vigenti e delle esigenze particolari per la cooperazione futura con partner stranieri con cui sono scambiate informazioni e elementi probatori, il presente regolamento non dovrebbe applicarsi alle autorità pubbliche di un paese terzo e alle organizzazioni internazionali che agiscono nel quadro della cooperazione o di accordi internazionali conclusi a livello dell'Unione o nazionale per la cooperazione delle autorità giudiziarie e di contrasto con l'Unione o con gli Stati membri, a condizione che il paese terzo o le organizzazioni internazionali pertinenti forniscano garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone. Se del caso, ciò può riguardare le attività di entità incaricate dai paesi terzi di svolgere compiti specifici a sostegno di tale cooperazione delle autorità giudiziarie e di contrasto. Tali quadri per la cooperazione o accordi sono stati istituiti bilateralmente tra Stati membri e paesi terzi o tra l'Unione europea, Europol e altre agenzie dell'Unione e paesi terzi e organizzazioni internazionali. Le autorità competenti per il controllo delle autorità giudiziarie e di contrasto ai sensi del presente regolamento dovrebbero valutare se tali quadri per la cooperazione o accordi internazionali includano garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone. Le autorità nazionali destinarie e le istituzioni, gli organi e gli organismi dell'Unione che si avvalgono di tali output nell'Unione, restano responsabili di garantire che il loro utilizzo sia conforme al diritto dell'Unione. In caso di revisione di tali accordi internazionali o di conclusione di nuovi accordi internazionali in futuro, le parti contraenti dovrebbero adoperarsi quanto più possibile per allineare tali accordi ai requisiti del presente regolamento.

- (23) È altresì opportuno che il presente regolamento si applichi alle istituzioni, agli organi e agli organismi dell'Unione quando agiscono in qualità di fornitori o deployer di un sistema di IA.

- (24) Se, e nella misura in cui, i sistemi di IA sono immessi sul mercato, messi in servizio o utilizzati con o senza modifica di tali sistemi per scopi militari, di difesa o di sicurezza nazionale, essi dovrebbero essere esclusi dall'ambito di applicazione del presente regolamento indipendentemente dal tipo di entità che svolge tali attività, ad esempio se si tratta di un'entità pubblica o privata. Per quanto riguarda gli scopi militari e di difesa, tale esclusione è giustificata sia dall'articolo 4, paragrafo 2, TUE sia dalle specificità della politica di difesa comune degli Stati membri e dell'Unione di cui al titolo V, capo 2, TUE che sono soggette al diritto internazionale pubblico, che costituisce pertanto il quadro giuridico più appropriato per la regolamentazione dei sistemi di IA nel contesto dell'uso letale della forza e di altri sistemi di IA nel contesto delle attività militari e di difesa. Per quanto riguarda le finalità di sicurezza nazionale, l'esclusione è giustificata sia dal fatto che la sicurezza nazionale resta di esclusiva competenza degli Stati membri ai sensi dell'articolo 4, paragrafo 2, TUE, sia dalla natura specifica e dalle esigenze operative delle attività di sicurezza nazionale, nonché dalle specifiche norme nazionali applicabili a tali attività. Tuttavia, se un sistema di IA sviluppato, immesso sul mercato, messo in servizio o utilizzato per scopi militari, di difesa o di sicurezza nazionale è usato al di fuori di tali finalità, in via temporanea o permanente, per altri scopi, ad esempio a fini civili o umanitari, per scopi di attività di contrasto o di sicurezza pubblica, tale sistema rientrerebbe nell'ambito di applicazione del presente regolamento. In tal caso, l'entità che utilizza il sistema di IA per finalità diverse da quelle militari, di difesa o di sicurezza nazionale dovrebbe garantire la conformità del sistema di IA al presente regolamento, a meno che il sistema non sia già conforme al presente regolamento. Rientrano nell'ambito di applicazione del presente regolamento i sistemi di IA immessi sul mercato o messi in servizio per una finalità esclusa, ossia militare, di difesa o di sicurezza nazionale, e per una o più finalità non escluse, ad esempio scopi civili o attività di contrasto, e i fornitori di tali sistemi dovrebbero garantire la conformità al presente regolamento. In tali casi, il fatto che un sistema di IA possa rientrare nell'ambito di applicazione del presente regolamento non dovrebbe incidere sulla possibilità per le entità che svolgono attività militari, di sicurezza nazionale e di difesa, indipendentemente dal tipo di entità che svolge tali attività, di utilizzare sistemi di IA per scopi di sicurezza nazionale, militari e di difesa, l'uso dei quali è escluso dall'ambito di applicazione del presente regolamento. Un sistema di IA immesso sul mercato per scopi civili o di attività di contrasto che è utilizzato con o senza modifiche a fini militari, di difesa o di sicurezza nazionale non dovrebbe rientrare nell'ambito di applicazione del presente regolamento, indipendentemente dal tipo di entità che svolge tali attività.

- (25) Il presente regolamento dovrebbe sostenere l'innovazione, rispettare la libertà della scienza e non dovrebbe pregiudicare le attività di ricerca e sviluppo. È pertanto necessario escludere dal suo ambito di applicazione i sistemi e i modelli di IA specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. È inoltre necessario garantire che il regolamento non incida altrimenti sulle attività scientifiche di ricerca e sviluppo relative ai sistemi o modelli di IA prima dell'immissione sul mercato o della messa in servizio. Per quanto riguarda le attività di ricerca, prova e sviluppo orientate ai prodotti relative ai sistemi o modelli di IA, le disposizioni del presente regolamento non dovrebbero nemmeno applicarsi prima che tali sistemi e modelli siano messi in servizio o immessi sul mercato. Tale esclusione non pregiudica l'obbligo di conformarsi al presente regolamento qualora un sistema di IA che rientra nell'ambito di applicazione del presente regolamento sia immesso sul mercato o messo in servizio in conseguenza di tale attività di ricerca e sviluppo, così come non pregiudica l'applicazione delle disposizioni sugli spazi di sperimentazione normativa per l'IA e sulle prove in condizioni reali. Inoltre, fatta salva l'esclusione dei sistemi di IA specificamente sviluppati e messi in servizio solo a scopo di ricerca e sviluppo in ambito scientifico, qualsiasi altro sistema di IA che possa essere utilizzato per lo svolgimento di qualsiasi attività di ricerca e sviluppo dovrebbe rimanere soggetto alle disposizioni del presente regolamento. In ogni caso, qualsiasi attività di ricerca e sviluppo dovrebbe essere svolta conformemente alle norme etiche e professionali riconosciute nell'ambito della ricerca scientifica e dovrebbe essere condotta conformemente al diritto dell'Unione applicabile.

- (26) Al fine di introdurre un insieme proporzionato ed efficace di regole vincolanti per i sistemi di IA è opportuno avvalersi di un approccio basato sul rischio definito in modo chiaro. Tale approccio dovrebbe adattare la tipologia e il contenuto di dette regole all'intensità e alla portata dei rischi che possono essere generati dai sistemi di IA. È pertanto necessario vietare determinate pratiche di IA inaccettabili, stabilire requisiti per i sistemi di IA ad alto rischio e obblighi per gli operatori pertinenti, nonché obblighi di trasparenza per determinati sistemi di IA.
- (27) Sebbene l'approccio basato sul rischio costituisca la base per un insieme proporzionato ed efficace di regole vincolanti, è importante ricordare gli orientamenti etici per un'IA affidabile del 2019 elaborati dall'AI HLEG indipendente nominato dalla Commissione. In tali orientamenti l'AI HLEG ha elaborato sette principi etici non vincolanti per l'IA che sono intesi a contribuire a garantire che l'IA sia affidabile ed eticamente valida. I sette principi comprendono: intervento e sorveglianza umani, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità. Fatti salvi i requisiti giuridicamente vincolanti del presente regolamento e di qualsiasi altra disposizione di diritto dell'Unione applicabile, tali orientamenti contribuiscono all'elaborazione di un'IA coerente, affidabile e antropocentrica, in linea con la Carta e con i valori su cui si fonda l'Unione. Secondo gli orientamenti dell'AI HLEG con "intervento e sorveglianza umani" si intende che i sistemi di IA sono sviluppati e utilizzati come strumenti al servizio delle persone, nel rispetto della dignità umana e dell'autonomia personale, e funzionano in modo da poter essere adeguatamente controllati e sorvegliati dagli esseri umani.

Con "robustezza tecnica e sicurezza" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire la robustezza nel caso di problemi e resilienza contro i tentativi di alterare l'uso o le prestazioni del sistema di IA in modo da consentire l'uso illegale da parte di terzi e ridurre al minimo i danni involontari. Con "vita privata e governance dei dati" si intende che i sistemi di IA sono sviluppati e utilizzati nel rispetto delle norme in materia di vita privata e protezione dei dati, elaborando al contempo dati che soddisfino livelli elevati in termini di qualità e integrità. Con "trasparenza" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i deployer delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti. Con "diversità, non discriminazione ed equità" si intende che i sistemi di IA sono sviluppati e utilizzati in modo da includere soggetti diversi e promuovere la parità di accesso, l'uguaglianza di genere e la diversità culturale, evitando nel contempo effetti discriminatori e pregiudizi ingiusti vietati dal diritto dell'Unione o nazionale. Con "benessere sociale e ambientale" si intende che i sistemi di IA sono sviluppati e utilizzati in modo sostenibile e rispettoso dell'ambiente e in modo da apportare benefici a tutti gli esseri umani, monitorando e valutando gli impatti a lungo termine sull'individuo, sulla società e sulla democrazia. L'applicazione di tali principi dovrebbe essere tradotta, ove possibile, nella progettazione e nell'utilizzo di modelli di IA. Essi dovrebbero in ogni caso fungere da base per l'elaborazione di codici di condotta a norma del presente regolamento. Tutti i portatori di interessi, compresi l'industria, il mondo accademico, la società civile e le organizzazioni di normazione, sono incoraggiati a tenere conto, se del caso, dei principi etici per lo sviluppo delle migliori pratiche e norme volontarie.

- (28) L'IA presenta, accanto a molti utilizzi benefici, la possibilità di essere utilizzata impropriamente e di fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale. Tali pratiche sono particolarmente dannose e abusive e dovrebbero essere vietate poiché sono contrarie ai valori dell'Unione relativi al rispetto della dignità umana, alla libertà, all'uguaglianza, alla democrazia e allo Stato di diritto e ai diritti fondamentali sanciti dalla Carta, compresi il diritto alla non discriminazione, alla protezione dei dati e alla vita privata e i diritti dei minori.

- (29) Le tecniche di manipolazione basate sull'IA possono essere utilizzate per persuadere le persone ad adottare comportamenti indesiderati o per indurle con l'inganno a prendere decisioni in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la libera scelta. L'immissione sul mercato, la messa in servizio o l'uso di determinati sistemi di IA con l'obiettivo o l'effetto di distorcere materialmente il comportamento umano, con il rischio di causare danni significativi, in particolare aventi effetti negativi sufficientemente importanti sulla salute fisica, psicologica o sugli interessi finanziari, sono particolarmente pericolosi e dovrebbero pertanto essere vietati. Tali sistemi di IA impiegano componenti subliminali quali stimoli audio, grafici e video che le persone non sono in grado di percepire poiché tali stimoli vanno al di là della percezione umana o altre tecniche manipolative o ingannevoli che sovvertono o pregiudicano l'autonomia, il processo decisionale o la libera scelta di una persona senza che sia consapevole di tali tecniche o, se ne è consapevole, senza che sia in grado di controllarle o resistervi o possa evitare l'inganno. Ciò potrebbe essere facilitato, ad esempio, da interfacce cervello-computer o dalla realtà virtuale, in quanto queste consentono un livello più elevato di controllo degli stimoli presentati alle persone, nella misura in cui possono distorcerne materialmente il comportamento in modo significativamente nocivo. In aggiunta, i sistemi di IA possono inoltre sfruttare in altro modo le vulnerabilità di una persona o di uno specifico gruppo di persone dovute all'età, a disabilità ai sensi della direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio¹³² o a una specifica situazione sociale o economica che potrebbe rendere tali persone più vulnerabili allo sfruttamento, come le persone che vivono in condizioni di povertà estrema e le minoranze etniche o religiose.

¹³² Direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi (GU L 151 del 7.6.2019, pag. 70).

Tali sistemi di IA possono essere immessi sul mercato, messi in servizio o utilizzati con l'obiettivo o l'effetto di distorcere materialmente il comportamento di una persona e in un modo che provochi o possa verosimilmente provocare a tale persona o a un'altra persona o gruppo di persone un danno significativo, compresi danni che possono essere accumulati nel tempo, e dovrebbero pertanto essere vietati. Potrebbe non essere possibile presumere che vi sia l'intenzione di distorcere il comportamento qualora la distorsione sia determinata da fattori esterni al sistema di IA, che sfuggono al controllo del fornitore o del deployer, ossia fattori che non possono essere ragionevolmente prevedibili e non possono quindi essere attenuati dal fornitore o dal deployer del sistema di IA. In ogni caso, non è necessario che il fornitore o il deployer abbiano l'intento di provocare un danno significativo, purché tale danno derivi da pratiche manipolative o di sfruttamento consentite dall'IA. Il divieto di tali pratiche di IA è complementare alle disposizioni contenute nella direttiva 2005/29/CE del Parlamento europeo e del Consiglio¹³³, in particolare le pratiche commerciali sleali che comportano danni economici o finanziari per i consumatori sono vietate in ogni circostanza, indipendentemente dal fatto che siano attuate attraverso sistemi di IA o in altro modo. I divieti di pratiche manipolative e di sfruttamento di cui al presente regolamento non dovrebbero pregiudicare le pratiche lecite nel contesto di trattamenti medici, quali il trattamento psicologico di una malattia mentale o la riabilitazione fisica, quando tali pratiche sono svolte conformemente al diritto applicabile e alle norme in ambito medico, ad esempio il consenso esplicito delle persone fisiche o dei loro rappresentanti legali. Inoltre, le pratiche commerciali comuni e legittime, ad esempio nel settore della pubblicità, che sono conformi alla normativa applicabile non dovrebbero essere considerate di per sé come pratiche consentite dall'IA manipolative o dannose.

¹³³ Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali delle imprese nei confronti dei consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio ("direttiva sulle pratiche commerciali sleali") (GU L 149 dell'11.6.2005, pag. 22).

- (30) Dovrebbero essere vietati i sistemi di categorizzazione biometrica basati sui dati biometrici di persone fisiche, quali il volto o le impronte digitali, per trarre deduzioni o inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona. Tale divieto non dovrebbe riguardare l'etichettatura, il filtraggio o la categorizzazione legali dei set di dati biometrici acquisiti in linea con il diritto dell'Unione o nazionale in funzione dei dati biometrici, come la selezione di immagini in base al colore dei capelli o degli occhi, che possono essere utilizzati, ad esempio, nel settore delle attività di contrasto.
- (31) I sistemi di IA che permettono ad attori pubblici o privati di attribuire un punteggio sociale alle persone fisiche possono portare a risultati discriminatori e all'esclusione di determinati gruppi. Possono inoltre ledere il diritto alla dignità e alla non discriminazione e i valori di uguaglianza e giustizia. Tali sistemi di IA valutano o classificano le persone fisiche o i gruppi di persone fisiche sulla base di vari punti di dati riguardanti il loro comportamento sociale in molteplici contesti o di caratteristiche personali o della personalità note, inferite o previste nell'arco di determinati periodi di tempo. Il punteggio sociale ottenuto da tali sistemi di IA può determinare un trattamento pregiudizievole o sfavorevole di persone fisiche o di interi gruppi in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, o a un trattamento pregiudizievole che risulta ingiustificato o sproporzionato rispetto alla gravità del loro comportamento sociale. I sistemi di IA che comportano tali pratiche inaccettabili di punteggio aventi risultati pregiudizievoli o sfavorevoli dovrebbero pertanto essere vietati. Tale divieto non dovrebbe pregiudicare le pratiche lecite di valutazione delle persone fisiche effettuate per uno scopo specifico in conformità del diritto dell'Unione e nazionale.

- (32) L'uso di sistemi di IA di identificazione biometrica remota "in tempo reale" delle persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto è particolarmente invasivo dei diritti e delle libertà delle persone interessate, nella misura in cui potrebbe avere ripercussioni sulla vita privata di un'ampia fetta della popolazione, farla sentire costantemente sotto sorveglianza e scoraggiare in maniera indiretta l'esercizio della libertà di riunione e di altri diritti fondamentali. Le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori. Tali possibili risultati distorti ed effetti discriminatori sono particolarmente importanti per quanto riguarda l'età, l'etnia, la razza, il sesso o le disabilità. L'immediatezza dell'impatto e le limitate opportunità di eseguire ulteriori controlli o apportare correzioni in relazione all'uso di tali sistemi che operano "in tempo reale" comportano inoltre un aumento dei rischi per quanto concerne i diritti e le libertà delle persone interessate nell'ambito delle attività di contrasto, o che sono da queste condizionate.

- (33) L'uso di tali sistemi a fini di attività di contrasto dovrebbe pertanto essere vietato, eccezion fatta per le situazioni elencate in modo esaustivo e definite rigorosamente, nelle quali l'uso è strettamente necessario per perseguire un interesse pubblico rilevante, la cui importanza prevale sui rischi. Tali situazioni comprendono la ricerca di determinate vittime di reato, comprese le persone scomparse, determinate minacce per la vita o l'incolumità fisica delle persone fisiche o un attacco terroristico nonché la localizzazione o l'identificazione degli autori o dei sospettati di reati elencati nell'allegato del presente regolamento qualora tali reati siano punibili nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà personale della durata massima di almeno quattro anni e sono definiti conformemente al diritto di tale Stato membro. Tale soglia per la pena o la misura di sicurezza privativa della libertà personale in conformità del diritto nazionale contribuisce a garantire che il reato sia sufficientemente grave da giustificare potenzialmente l'uso di sistemi di identificazione biometrica remota "in tempo reale". Inoltre, l'elenco dei reati di cui all'allegato del presente regolamento è basato sui 32 reati elencati nella decisione quadro 2002/584/GAI del Consiglio¹³⁴, tenendo conto che alcuni reati risultano più pertinenti di altri, poiché il grado di necessità e proporzionalità del ricorso all'identificazione biometrica remota "in tempo reale" potrebbe essere prevedibilmente molto variabile per quanto concerne il perseguimento pratico della localizzazione o dell'identificazione nei confronti di un autore o un sospettato dei vari reati elencati e con riguardo alle possibili differenze in termini di gravità, probabilità e portata del danno o delle eventuali conseguenze negative.

¹³⁴ Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri (GU L 190 del 18.7.2002, pag. 1).

Una minaccia imminente per la vita o l'incolumità fisica delle persone fisiche potrebbe anche derivare da un grave danneggiamento dell'infrastruttura critica quale definita all'articolo 2, punto 4, della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio¹³⁵, ove il danneggiamento o la distruzione di tale infrastruttura critica possa comportare una minaccia imminente per la vita o l'integrità fisica di una persona, anche in ragione di un grave danno alla fornitura di forniture di base alla popolazione o all'esercizio della funzione essenziale dello Stato. Il presente regolamento dovrebbe altresì preservare la capacità delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo di svolgere controlli d'identità in presenza della persona interessata, conformemente alle condizioni stabilite per tali controlli dal diritto dell'Unione e nazionale. In particolare, le autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo dovrebbero poter utilizzare i sistemi di informazione, conformemente al diritto dell'Unione o nazionale, per identificare le persone che, durante un controllo d'identità, rifiutano di essere identificate o non sono in grado di dichiarare o dimostrare la loro identità, senza essere tenute, a norma del presente regolamento, a ottenere un'autorizzazione preventiva. Potrebbe trattarsi, ad esempio, di una persona coinvolta in un reato che, a causa di un incidente o di un problema di salute, non vuole rivelare la propria identità alle autorità di contrasto o non è in grado di farlo.

¹³⁵ Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio (GU L 333 del 27.12.2022, pag. 164).

- (34) Al fine di garantire che tali sistemi siano utilizzati in modo responsabile e proporzionato, è altresì importante stabilire che, in ciascuna delle situazioni elencate in modo esaustivo e definite rigorosamente, è opportuno tener conto di taluni elementi, in particolare per quanto riguarda la natura della situazione all'origine della richiesta e le conseguenze dell'uso per i diritti e le libertà di tutte le persone interessate, nonché le tutele e le condizioni previste per l'uso. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto dovrebbe inoltre essere impiegato solo per confermare l'identità della persona specificamente interessata e dovrebbe essere limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale, con particolare riguardo a indicazioni o elementi probatori relativi a minacce, vittime o autori di reati. L'uso del sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico dovrebbe essere autorizzato solo se l'autorità di contrasto pertinente ha completato una valutazione d'impatto sui diritti fondamentali e, salvo disposizione contraria del presente regolamento, ha registrato il sistema nella banca dati di cui al presente regolamento. La banca dati di riferimento delle persone dovrebbe risultare adeguata per ogni caso d'uso in ciascuna delle situazioni di cui sopra.

- (35) È opportuno subordinare ogni uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a un'autorizzazione esplicita e specifica da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente di uno Stato membro la cui decisione sia vincolante. Tale autorizzazione dovrebbe, in linea di principio, essere ottenuta prima dell'uso del sistema di IA al fine di identificare una o più persone. Eccezioni a tale regola dovrebbero essere ammesse in situazioni di urgenza debitamente giustificate, vale a dire le situazioni in cui la necessità di utilizzare i sistemi interessati è tale da far sì che sia effettivamente e oggettivamente impossibile ottenere un'autorizzazione prima di iniziare a utilizzare il sistema di IA. In tali situazioni di urgenza, è opportuno limitare l'uso del sistema di IA al minimo indispensabile e subordinarlo a tutele e condizioni adeguate, come stabilito dal diritto nazionale e specificato nel contesto di ogni singolo caso d'uso urgente dall'autorità di contrasto stessa. In tali situazioni, inoltre, l'autorità di contrasto dovrebbe richiedere tale autorizzazione, indicando contestualmente i motivi per cui non ha potuto richiederla prima, senza indebito ritardo e al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso dei sistemi di identificazione biometrica "in tempo reale" collegati a tale autorizzazione dovrebbe essere interrotto con effetto immediato e tutti i dati relativi a tale uso dovrebbero essere eliminati e cancellati. Tali dati comprendono i dati di input acquisiti direttamente da un sistema di IA nel corso dell'uso di tale sistema, nonché i risultati e gli output dell'uso connessi a tale autorizzazione. Non dovrebbero includere gli input acquisiti legalmente in conformità di altre disposizioni del diritto dell'Unione o nazionale. In ogni caso, nessuna decisione che produca effetti giuridici negativi su una persona dovrebbe essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota.

- (36) Affinché svolgano i loro compiti conformemente alle prescrizioni del presente regolamento e alle norme nazionali, è opportuno notificare alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati ogni uso del sistema di identificazione biometrica "in tempo reale". Le autorità di vigilanza del mercato e le autorità nazionali per la protezione dei dati che sono state notificate dovrebbero presentare alla Commissione una relazione annuale sull'uso dei sistemi di identificazione biometrica "in tempo reale".
- (37) È altresì opportuno prevedere, nell'ambito del quadro esaustivo stabilito dal presente regolamento, che tale uso nel territorio di uno Stato membro in conformità del presente regolamento sia possibile solo nel caso e nella misura in cui lo Stato membro interessato abbia deciso di prevedere espressamente la possibilità di autorizzare tale uso nelle regole dettagliate del proprio diritto nazionale. Gli Stati membri restano di conseguenza liberi, a norma del presente regolamento, di non prevedere affatto tale possibilità o di prevederla soltanto per alcuni degli obiettivi idonei a giustificare l'uso autorizzato di cui nel presente regolamento. Tali regole nazionali dovrebbero essere notificate alla Commissione entro 30 giorni dalla loro adozione.

(38) L'uso di sistemi di IA per l'identificazione biometrica remota "in tempo reale" di persone fisiche in spazi accessibili al pubblico a fini di attività di contrasto comporta necessariamente il trattamento di dati biometrici. Le regole del presente regolamento che, fatte salve alcune eccezioni, vietano tale uso, e che sono basate sull'articolo 16 TFUE, dovrebbero applicarsi come *lex specialis* rispetto alle regole sul trattamento dei dati biometrici di cui all'articolo 10 della direttiva (UE) 2016/680, disciplinando quindi in modo esaustivo tale uso e il trattamento dei dati biometrici interessati. L'uso e il trattamento di cui sopra dovrebbero pertanto essere possibili solo nella misura in cui siano compatibili con il quadro stabilito dal presente regolamento, senza che al di fuori di tale quadro sia prevista la possibilità, per le autorità competenti, quando agiscono a fini di attività di contrasto, di utilizzare tali sistemi e trattare tali dati in connessione con tali attività per i motivi di cui all'articolo 10 della direttiva (UE) 2016/680. In tale contesto, il presente regolamento non è inteso a fornire la base giuridica per il trattamento dei dati personali a norma dell'articolo 8 della direttiva (UE) 2016/680. Tuttavia, l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini diversi dalle attività di contrasto, anche da parte delle autorità competenti, non dovrebbe rientrare nel quadro specifico stabilito dal presente regolamento in relazione a tale uso a fini di attività di contrasto. Tale uso a fini diversi dalle attività di contrasto non dovrebbe pertanto essere subordinato all'obbligo di un'autorizzazione a norma del presente regolamento e delle regole dettagliate applicabili del diritto nazionale che possono dare attuazione a tale autorizzazione.

- (39) Qualsiasi trattamento di dati biometrici e di altri dati personali interessati dall'uso di sistemi di IA a fini di identificazione biometrica, diverso da quello connesso all'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto disciplinato dal presente regolamento, dovrebbe continuare a soddisfare tutti i requisiti derivanti dall'articolo 10 della direttiva (UE) 2016/680. Per fini diversi dalle attività di contrasto, l'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 e l'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725 vietano il trattamento di dati biometrici fatte salve limitate eccezioni previste da tali articoli. Nell'applicazione dell'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, l'uso dell'identificazione biometrica remota a fini diversi dalle attività di contrasto è già stato oggetto di decisioni di divieto da parte delle autorità nazionali per la protezione dei dati.

- (40) A norma dell'articolo 6 bis del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, l'Irlanda non è vincolata dalle regole stabilite all'articolo 5, paragrafo 1, primo comma, lettera g), nella misura in cui si applica all'uso di sistemi di categorizzazione biometrica per le attività nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, all'articolo 5, paragrafo 1, primo comma, lettera d), nella misura in cui si applica all'uso dei sistemi di IA contemplati da tale disposizione, all'articolo 5, paragrafo 1, primo comma, lettera h), paragrafi da 2 a 6, e all'articolo 26, paragrafo 10, del presente regolamento, adottate in base all'articolo 16 TFUE, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE, laddove l'Irlanda non sia vincolata da regole che disciplinano forme di cooperazione giudiziaria in materia penale o di cooperazione di polizia nell'ambito delle quali devono essere rispettate le disposizioni stabilite in base all'articolo 16 TFUE.

- (41) A norma degli articoli 2 e 2 bis del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al TFUE, la Danimarca non è vincolata dalle regole stabilite all'articolo 5, paragrafo 1, primo comma, lettera g), nella misura in cui si applica all'uso di sistemi di categorizzazione biometrica per le attività nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, all'articolo 5, paragrafo 1, primo comma, lettera d), nella misura in cui si applica all'uso dei sistemi di IA contemplati da tale disposizione, all'articolo 5, paragrafo 1, primo comma, lettera h), paragrafi da 2 a 6, e all'articolo 26, paragrafo 10, del presente regolamento, adottate in base all'articolo 16 TFUE, che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE, né è soggetta alla loro applicazione.

- (42) In linea con la presunzione di innocenza, le persone fisiche nell'Unione dovrebbero sempre essere giudicate in base al loro comportamento effettivo. Le persone fisiche non dovrebbero mai essere giudicate sulla base di un comportamento previsto dall'IA basato unicamente sulla profilazione, sui tratti della personalità o su caratteristiche quali la cittadinanza, il luogo di nascita, il luogo di residenza, il numero di figli, il livello di indebitamento o il tipo di automobile, senza che vi sia un ragionevole sospetto che la persona sia coinvolta in un'attività criminosa sulla base di fatti oggettivi verificabili e senza una valutazione umana al riguardo. Pertanto, dovrebbero essere vietate le valutazioni del rischio effettuate in relazione a persone fisiche intese a determinare la probabilità che queste ultime commettano un reato o volte a prevedere il verificarsi di un reato effettivo o potenziale unicamente sulla base della loro profilazione o della valutazione dei loro tratti della personalità e delle loro caratteristiche. In ogni caso, tale divieto non fa riferimento né riguarda l'analisi del rischio che non è basata sulla profilazione delle persone o sui tratti della personalità e sulle caratteristiche delle persone, come i sistemi di IA che utilizzano l'analisi dei rischi per valutare il rischio di frode finanziaria da parte di imprese sulla base di transazioni sospette o di strumenti di analisi del rischio per prevedere la probabilità di localizzazione di stupefacenti o merci illecite da parte delle autorità doganali, ad esempio sulla base di rotte di traffico conosciute.
- (43) L'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso dovrebbero essere vietati, in quanto tale pratica accresce il senso di sorveglianza di massa e può portare a gravi violazioni dei diritti fondamentali, compreso il diritto alla vita privata.

- (44) Sussistono serie preoccupazioni in merito alla base scientifica dei sistemi di IA volti a identificare o inferire emozioni, in particolare perché l'espressione delle emozioni varia notevolmente in base alle culture e alle situazioni e persino in relazione a una stessa persona. Tra le principali carenze di tali sistemi figurano la limitata affidabilità, la mancanza di specificità e la limitata generalizzabilità. Pertanto, i sistemi di IA che identificano o inferiscono emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici possono portare a risultati discriminatori e possono essere invasivi dei diritti e delle libertà delle persone interessate. Considerando lo squilibrio di potere nel contesto del lavoro o dell'istruzione, combinato con la natura invasiva di tali sistemi, questi ultimi potrebbero determinare un trattamento pregiudizievole o sfavorevole di talune persone fisiche o di interi gruppi di persone fisiche. È pertanto opportuno vietare l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA destinati a essere utilizzati per rilevare lo stato emotivo delle persone in situazioni relative al luogo di lavoro e all'istruzione. Tale divieto non dovrebbe riguardare i sistemi di IA immessi sul mercato esclusivamente per motivi medici o di sicurezza, come i sistemi destinati all'uso terapeutico.
- (45) Il presente regolamento non dovrebbe incidere sulle pratiche vietate dal diritto dell'Unione, ivi incluso dal diritto in materia di protezione dei dati, non discriminazione, protezione dei consumatori e concorrenza.

- (46) È opportuno che i sistemi di IA ad alto rischio siano immessi sul mercato dell'Unione, messi in servizio o utilizzati solo se soddisfano determinati requisiti obbligatori. Tali requisiti dovrebbero garantire che i sistemi di IA ad alto rischio disponibili nell'Unione o i cui output sono altrimenti utilizzati nell'Unione non presentino rischi inaccettabili per interessi pubblici importanti dell'Unione, come riconosciuti e tutelati dal diritto dell'Unione. In base al nuovo quadro legislativo, come chiarito nella comunicazione della Commissione "La "Guida blu" all'attuazione della normativa UE sui prodotti 2022"¹³⁶, la regola generale è che più di un atto giuridico della normativa di armonizzazione dell'Unione, come i regolamenti (UE) 2017/745¹³⁷ e (UE) 2017/746¹³⁸ del Parlamento europeo e del Consiglio o la direttiva n. 2006/42/CE del Parlamento europeo e del Consiglio¹³⁹, può essere applicabile a un solo prodotto, poiché quest'ultimo può essere messo a disposizione o messo in servizio solo se risulta conforme a tutta la normativa di armonizzazione dell'Unione applicabile. Al fine di garantire la coerenza ed evitare oneri amministrativi o costi non necessari, i fornitori di un prodotto contenente uno o più sistemi di IA ad alto rischio cui si applicano i requisiti del presente regolamento e della normativa di armonizzazione dell'Unione elencata in un allegato del presente regolamento dovrebbero avere flessibilità per quanto riguarda le decisioni operative sui modi per garantire in modo ottimale la conformità di un prodotto contenente uno o più sistemi di IA a tutti i requisiti applicabili della normativa di armonizzazione dell'Unione. È opportuno limitare i sistemi di IA identificati come ad alto rischio a quelli che hanno un impatto nocivo significativo sulla salute, la sicurezza e i diritti fondamentali delle persone nell'Unione, e tale limitazione dovrebbe ridurre al minimo eventuali potenziali restrizioni al commercio internazionale.

¹³⁶ GU C 247 del 29.6.2022, pag. 1.

¹³⁷ Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1).

¹³⁸ Regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici *in vitro* e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

¹³⁹ Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24).

- (47) I sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati.

- (48) La portata dell'impatto negativo del sistema di IA sui diritti fondamentali protetti dalla Carta è di particolare rilevanza ai fini della classificazione di un sistema di IA tra quelli ad alto rischio. Tali diritti comprendono il diritto alla dignità umana, il rispetto della vita privata e della vita familiare, la protezione dei dati personali, la libertà di espressione e di informazione, la libertà di riunione e di associazione e il diritto alla non discriminazione, il diritto all'istruzione, la protezione dei consumatori, i diritti dei lavoratori, i diritti delle persone con disabilità, l'uguaglianza di genere, i diritti di proprietà intellettuale, il diritto a un ricorso effettivo e a un giudice imparziale, i diritti della difesa e la presunzione di innocenza e il diritto a una buona amministrazione. Oltre a tali diritti, è importante sottolineare il fatto che i minori godono di diritti specifici sanciti dall'articolo 24 della Carta e dalla Convenzione delle Nazioni Unite sui diritti dell'infanzia e dell'adolescenza, ulteriormente sviluppati nell'osservazione generale n. 25 della Convenzione delle Nazioni Unite dell'infanzia e dell'adolescenza per quanto riguarda l'ambiente digitale, che prevedono la necessità di tenere conto delle loro vulnerabilità e di fornire la protezione e l'assistenza necessarie al loro benessere. È altresì opportuno tenere in considerazione, nel valutare la gravità del danno che un sistema di IA può provocare, anche in relazione alla salute e alla sicurezza delle persone, il diritto fondamentale a un livello elevato di protezione dell'ambiente sancito dalla Carta e attuato nelle politiche dell'Unione.

- (49) Per quanto riguarda i sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti o sistemi o che sono essi stessi prodotti o sistemi che rientrano nell'ambito di applicazione del regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio¹⁴⁰, del regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio¹⁴¹, del regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio¹⁴², della direttiva 2014/90/UE del Parlamento europeo e del Consiglio¹⁴³, della direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio¹⁴⁴,

¹⁴⁰ Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72).

¹⁴¹ Regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1).

¹⁴² Regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio, del 15 gennaio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli (GU L 60 del 2.3.2013, pag. 52).

¹⁴³ Direttiva 2014/90/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sull'equipaggiamento marittimo e che abroga la direttiva 96/98/CE del Consiglio (GU L 257 del 28.8.2014, pag. 146).

¹⁴⁴ Direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, relativa all'interoperabilità del sistema ferroviario dell'Unione europea (GU L 138 del 26.5.2016, pag. 44).

del regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio¹⁴⁵, del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio¹⁴⁶, e del regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio¹⁴⁷, è opportuno modificare i suddetti atti per garantire che, nell'adottare qualsiasi atto delegato o di esecuzione pertinente sulla base di tali atti, la Commissione tenga conto, sulla base delle specificità tecniche e normative di ciascun settore e senza interferire con i vigenti meccanismi di governance, valutazione della conformità e applicazione e con le autorità da essi stabilite, dei requisiti obbligatori sanciti dal presente regolamento.

¹⁴⁵ Regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE (GU L 151 del 14.6.2018, pag. 1).

¹⁴⁶ Regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1).

¹⁴⁷ Regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010, (UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011, (UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012, (UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione (GU L 325 del 16.12.2019, pag. 1).

- (50) Per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, macchine, giocattoli, ascensori, apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici, dispositivi medico-diagnostici *in vitro*, veicoli automobilistici e aeronautici.
- (51) La classificazione di un sistema di IA come ad alto rischio a norma del presente regolamento non dovrebbe necessariamente significare che il prodotto il cui componente di sicurezza è il sistema di IA, o il sistema di IA stesso in quanto prodotto, sia considerato "ad alto rischio" in base ai criteri stabiliti nella pertinente normativa di armonizzazione dell'Unione che si applica al prodotto. Ciò vale, in particolare, per i regolamenti (UE) 2017/745 e (UE) 2017/746, in cui è prevista una valutazione della conformità da parte di terzi per i prodotti a medio rischio e ad alto rischio.

- (52) Per quanto riguarda i sistemi di IA indipendenti, ossia i sistemi di IA ad alto rischio diversi da quelli che sono componenti di sicurezza dei prodotti o che sono essi stessi prodotti, è opportuno classificarli come ad alto rischio se, alla luce della loro finalità prevista, presentano un alto rischio di pregiudicare la salute e la sicurezza o i diritti fondamentali delle persone, tenendo conto sia della gravità del possibile danno sia della probabilità che si verifichi, e sono utilizzati in una serie di settori specificamente predefiniti indicati nel presente regolamento. L'identificazione di tali sistemi si basa sulla stessa metodologia e sui medesimi criteri previsti anche per eventuali future modifiche dell'elenco dei sistemi di IA ad alto rischio che la Commissione dovrebbe avere il potere di adottare, mediante atti delegati, per tenere conto del rapido ritmo dello sviluppo tecnologico nonché dei potenziali cambiamenti nell'uso dei sistemi di IA.

- (53) È altresì importante chiarire che possono esservi casi specifici in cui i sistemi di IA riferiti a settori predefiniti indicati nel presente regolamento non comportano un rischio significativo di pregiudicare gli interessi giuridici tutelati nell'ambito di tali settori in quanto non influenzano materialmente il processo decisionale né pregiudicano tali interessi in modo sostanziale. Ai fini del presente regolamento, un sistema di IA che non influenza materialmente l'esito del processo decisionale dovrebbe essere inteso come un sistema di IA che non ha un impatto sulla sostanza, e quindi sull'esito, del processo decisionale, sia esso umano o automatizzato. Un sistema di IA che non influenza materialmente l'esito del processo decisionale potrebbe includere situazioni in cui sono soddisfatte una o più delle seguenti condizioni. La prima di tali condizioni dovrebbe essere che il sistema di IA sia destinato a svolgere un compito procedurale ristretto, come un sistema di IA che trasforma dati non strutturati in dati strutturati, un sistema di IA che classifica i documenti in entrata per categorie o un sistema di IA utilizzato per rilevare duplicati tra un gran numero di applicazioni. Tali compiti sono di natura così ristretta e limitata da comportare solo rischi limitati che non aumentano con l'uso di un sistema di IA in un contesto elencato come uso ad alto rischio in un allegato del presente regolamento. La seconda condizione dovrebbe essere che il compito svolto dal sistema di IA sia inteso a migliorare il risultato di un'attività umana precedentemente completata che può essere pertinente ai fini degli usi ad alto rischio elencati nell' allegato del presente regolamento. Tenuto conto di tali caratteristiche, il sistema di IA fornisce solo un livello aggiuntivo a un'attività umana con conseguente riduzione del rischio. Tale condizione si applicherebbe, ad esempio, ai sistemi di IA destinati a migliorare il linguaggio utilizzato in documenti redatti in precedenza, ad esempio in relazione al tono professionale, allo stile accademico del linguaggio o allineando il testo a una determinata comunicazione di marchio. La terza condizione dovrebbe essere che il sistema di IA sia inteso a individuare modelli decisionali o deviazioni da modelli decisionali precedenti.

Il rischio sarebbe ridotto in quanto l'uso del sistema di IA segue una valutazione umana precedentemente completata che non è destinato a sostituire o influenzare, senza un'adeguata revisione umana. Tali sistemi di IA comprendono, ad esempio, quelli che, dato un determinato modello di valutazione di un insegnante, possono essere utilizzati per verificare *ex post* se l'insegnante possa essersi discostato dal modello di valutazione in modo da segnalare potenziali incongruenze o anomalie. La quarta condizione dovrebbe essere che il sistema di IA sia destinato a svolgere un compito che è solo preparatorio rispetto a una valutazione pertinente ai fini dei sistemi di IA elencati in un allegato del presente regolamento, e pertanto la probabilità che l'output del sistema presenti un rischio per la valutazione posteriore è molto ridotto. Tale condizione riguarda, in particolare, soluzioni intelligenti per la gestione dei fascicoli, che comprendono varie funzioni quali l'indicizzazione, la ricerca, l'elaborazione testuale e vocale o il collegamento dei dati ad altre fonti di dati, o i sistemi di IA utilizzati per la traduzione di documenti iniziali. In ogni caso, è opportuno ritenere che i sistemi di IA utilizzati ad alto rischio elencati nell'allegato del presente regolamento comportino rischi significativi di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche se il sistema di IA implica la profilazione ai sensi dell'articolo 4, punto 4, del regolamento (UE) 2016/679, o dell'articolo 3, punto 4, della direttiva (UE) 2016/680 o dell'articolo 3, punto 5, del regolamento (UE) 2018/1725. Al fine di garantire la tracciabilità e la trasparenza, un fornitore che ritiene che un sistema di IA non sia ad alto rischio sulla base delle condizioni di cui sopra dovrebbe redigere la documentazione relativa alla valutazione prima che tale sistema sia immesso sul mercato o messo in servizio e dovrebbe fornire tale documentazione alle autorità nazionali competenti su richiesta. Tale fornitore dovrebbe essere tenuto a registrare il sistema di IA nella banca dati dell'UE istituita a norma del presente regolamento. Al fine di fornire ulteriori orientamenti per l'attuazione pratica delle condizioni alle quali i sistemi di IA elencati in un allegato del presente regolamento sono, in via eccezionale, non ad alto rischio, la Commissione, previa consultazione del consiglio per l'IA, dovrebbe fornire orientamenti che specifichino tale attuazione pratica completati da un elenco completo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e casi d'uso che non lo sono.

- (54) Poiché i dati biometrici costituiscono una categoria particolare di dati personali, è opportuno classificare come ad alto rischio diversi casi di uso critico di sistemi biometrici, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale. Le inesattezze di carattere tecnico dei sistemi di IA destinati all'identificazione biometrica remota delle persone fisiche possono determinare risultati distorti e comportare effetti discriminatori. Il rischio di tali risultati distorti ed effetti discriminatori è particolarmente importante per quanto riguarda l'età, l'etnia, la razza, il sesso o le disabilità. I sistemi destinati all'identificazione biometrica remota dovrebbero pertanto essere classificati come ad alto rischio in considerazione dei rischi che comportano. Tale classificazione esclude i sistemi di IA destinati a essere utilizzati per la verifica biometrica, inclusa l'autenticazione, la cui unica finalità è confermare che una determinata persona fisica è chi dice di essere e confermare l'identità di una persona fisica al solo scopo di accedere a un servizio, sbloccare un dispositivo o disporre dell'accesso sicuro a locali. Inoltre, è opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti a norma dell'articolo 9, paragrafo 1, del regolamento (UE) 2016/679 sulla base di dati biometrici, nella misura in cui non sono vietati a norma del presente regolamento, e i sistemi di riconoscimento delle emozioni che non sono vietati a norma del presente regolamento. I sistemi biometrici destinati a essere utilizzati al solo scopo di consentire la cibersicurezza e le misure di protezione dei dati personali non dovrebbero essere considerati sistemi di IA ad alto rischio.

- (55) Per quanto riguarda la gestione e il funzionamento delle infrastrutture critiche, è opportuno classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati come componenti di sicurezza ai fini della gestione e del funzionamento delle infrastrutture digitali critiche di cui all'allegato, punto 8, della direttiva (UE) 2022/2557, del traffico stradale nonché della fornitura di acqua, gas, riscaldamento ed elettricità, in quanto un loro guasto o malfunzionamento può mettere a rischio la vita e la salute di un grande numero di persone e provocare perturbazioni significative del normale svolgimento delle attività sociali ed economiche. I componenti di sicurezza delle infrastrutture critiche, comprese le infrastrutture digitali critiche, sono sistemi utilizzati per proteggere direttamente l'integrità fisica delle infrastrutture critiche ovvero la salute e la sicurezza delle persone e dei beni ma che non sono necessari per il funzionamento del sistema. Un guasto o malfunzionamento di tali componenti potrebbe comportare direttamente rischi per l'integrità fisica delle infrastrutture critiche e quindi per la salute e la sicurezza delle persone e dei beni. I componenti destinati a essere utilizzati esclusivamente a fini di cibersicurezza non dovrebbero essere considerati componenti di sicurezza. Tra gli esempi di componenti di sicurezza di tali infrastrutture critiche possono rientrare i sistemi di monitoraggio della pressione idrica o sistemi di controllo degli incendi nei centri di cloud computing.

- (56) La diffusione dei sistemi di IA nell'istruzione è importante per promuovere un'istruzione e una formazione digitali di alta qualità e per consentire a tutti i discenti e gli insegnanti di acquisire e condividere le competenze e le abilità digitali necessarie, compresa l'alfabetizzazione mediatica, e il pensiero critico, per partecipare attivamente all'economia, alla società e ai processi democratici. Tuttavia, i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento delle persone, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento. Se progettati e utilizzati in modo inadeguato, tali sistemi possono essere particolarmente intrusivi e violare il diritto all'istruzione e alla formazione, nonché il diritto alla non discriminazione, e perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale.

- (57) Anche i sistemi di IA utilizzati nel settore dell'occupazione, nella gestione dei lavoratori e nell'accesso al lavoro autonomo, in particolare per l'assunzione e la selezione delle persone, per l'adozione di decisioni riguardanti le condizioni del rapporto di lavoro la promozione e la cessazione dei rapporti contrattuali di lavoro, per l'assegnazione dei compiti sulla base dei comportamenti individuali, dei tratti o delle caratteristiche personali e per il monitoraggio o la valutazione delle persone nei rapporti contrattuali legati al lavoro, dovrebbero essere classificati come sistemi ad alto rischio, in quanto tali sistemi possono avere un impatto significativo sul futuro di tali persone in termini di prospettive di carriera e sostentamento e di diritti dei lavoratori. I pertinenti rapporti contrattuali di lavoro dovrebbero coinvolgere, in modo significativo, i dipendenti e le persone che forniscono servizi tramite piattaforme, come indicato nel programma di lavoro annuale della Commissione per il 2021. Durante tutto il processo di assunzione, nonché ai fini della valutazione e della promozione delle persone o del proseguimento dei rapporti contrattuali legati al lavoro, tali sistemi possono perpetuare modelli storici di discriminazione, ad esempio nei confronti delle donne, di talune fasce di età, delle persone con disabilità o delle persone aventi determinate origini razziali o etniche o un determinato orientamento sessuale. I sistemi di IA utilizzati per monitorare le prestazioni e il comportamento di tali persone possono inoltre comprometterne i diritti fondamentali in materia di protezione dei dati e vita privata.

- (58) Un altro settore in cui l'utilizzo dei sistemi di IA merita particolare attenzione è l'accesso ad alcuni servizi e prestazioni essenziali, pubblici e privati, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, e la fruizione di tali servizi. In particolare, le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, vale a dire servizi sanitari, prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia, gli infortuni sul lavoro, la dipendenza o la vecchiaia e la perdita di occupazione e l'assistenza sociale e abitativa, sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità responsabili. I sistemi di IA, se utilizzati per determinare se tali prestazioni e servizi dovrebbero essere concessi, negati, ridotti, revocati o recuperati dalle autorità, compreso se i beneficiari hanno legittimamente diritto a tali prestazioni o servizi, possono avere un impatto significativo sul sostentamento delle persone e violare i loro diritti fondamentali, quali il diritto alla protezione sociale, alla non discriminazione, alla dignità umana o a un ricorso effettivo e dovrebbero pertanto essere classificati come sistemi ad alto rischio. Cionondimeno, il presente regolamento non dovrebbe ostacolare lo sviluppo e l'utilizzo di approcci innovativi nella pubblica amministrazione, che trarrebbero beneficio da un uso più ampio di sistemi di IA conformi e sicuri, a condizione che tali sistemi non comportino un rischio alto per le persone fisiche e giuridiche.

È inoltre opportuno classificare i sistemi di IA utilizzati per valutare il merito di credito o l'affidabilità creditizia delle persone fisiche come sistemi di IA ad alto rischio, in quanto determinano l'accesso di tali persone alle risorse finanziarie o a servizi essenziali quali l'alloggio, l'elettricità e i servizi di telecomunicazione. I sistemi di IA utilizzati a tali fini possono portare alla discriminazione fra persone o gruppi e possono perpetuare modelli storici di discriminazione, come quella basata sull'origine razziale o etnica, sul genere, sulle disabilità, sull'età o sull'orientamento sessuale, o possono dar vita a nuove forme di impatti discriminatori. Tuttavia, i sistemi di IA previsti dal diritto dell'Unione al fine di individuare frodi nell'offerta di servizi finanziari e a fini prudenziali per calcolare i requisiti patrimoniali degli enti creditizi e delle imprese assicurative non dovrebbero essere considerati ad alto rischio ai sensi del presente regolamento. Inoltre, anche i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi in relazione alle persone fisiche per assicurazioni sulla vita e assicurazioni sanitarie possono avere un impatto significativo sul sostentamento delle persone e, se non debitamente progettati, sviluppati e utilizzati, possono violare i loro diritti fondamentali e comportare gravi conseguenze per la vita e la salute delle persone, tra cui l'esclusione finanziaria e la discriminazione. Infine, è opportuno classificare come ad alto rischio anche i sistemi di IA utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, anche da parte di polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza in quanto prendono decisioni in situazioni molto critiche per la vita e la salute delle persone e per i loro beni.

- (59) Tenuto conto del loro ruolo e della loro responsabilità, le azioni delle autorità di contrasto che prevedono determinati usi dei sistemi di IA sono caratterizzate da un livello significativo di squilibrio di potere e possono portare alla sorveglianza, all'arresto o alla privazione della libertà di una persona fisica, come pure avere altri impatti negativi sui diritti fondamentali garantiti nella Carta. In particolare, il sistema di IA, se non è addestrato con dati di elevata qualità, se non soddisfa requisiti adeguati in termini di prestazione, accuratezza o robustezza, o se non è adeguatamente progettato e sottoposto a prova prima di essere immesso sul mercato o altrimenti messo in servizio, può individuare le persone in modo discriminatorio o altrimenti errato o ingiusto. Potrebbe inoltre essere ostacolato l'esercizio di importanti diritti procedurali fondamentali, quali il diritto a un ricorso effettivo e a un giudice imparziale, nonché i diritti della difesa e la presunzione di innocenza, in particolare nel caso in cui tali sistemi di IA non siano sufficientemente trasparenti, spiegabili e documentati. È pertanto opportuno classificare come ad alto rischio, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale, una serie di sistemi di IA destinati a essere utilizzati nel contesto delle attività di contrasto, in cui l'accuratezza, l'affidabilità e la trasparenza risultano particolarmente importanti per evitare impatti negativi, mantenere la fiducia dei cittadini e garantire la responsabilità e mezzi di ricorso efficaci.

In considerazione della natura delle attività e dei rischi a esse connessi, tra tali sistemi di IA ad alto rischio è opportuno includere, in particolare, i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto, o per loro conto, o dagli organi o organismi dell'Unione a sostegno delle autorità di contrasto per valutare il rischio per una persona fisica di diventare vittima di reati, come poligrafi e strumenti analoghi, valutare l'affidabilità degli elementi probatori nel corso dell'accertamento e del perseguimento di reati, e, nella misura in cui non è vietato a norma del presente regolamento, determinare il rischio di reato o recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche, ma anche della valutazione dei tratti e delle caratteristiche della personalità o del comportamento criminale pregresso delle persone fisiche o dei gruppi, ai fini della profilazione nel corso dell'indagine, dell'accertamento e del perseguimento di reati. I sistemi di IA specificamente destinati a essere utilizzati per procedimenti amministrativi dalle autorità fiscali e doganali, come pure dalle unità di informazione finanziaria che svolgono compiti amministrativi di analisi delle informazioni conformemente al diritto dell'Unione in materia di antiriciclaggio, non dovrebbero essere classificati come sistemi di IA ad alto rischio utilizzati dalle autorità di contrasto a fini di prevenzione, accertamento, indagine e perseguimento di reati. L'utilizzo degli strumenti di IA da parte delle autorità di contrasto e delle altre pertinenti autorità non dovrebbe diventare un fattore di disuguaglianza o esclusione. L'impatto dell'utilizzo degli strumenti di IA sul diritto alla difesa degli indagati non dovrebbe essere ignorato, in particolare la difficoltà di ottenere informazioni significative sul funzionamento di tali sistemi e la difficoltà che ne risulta nel confutarne i risultati in tribunale, in particolare per le persone fisiche sottoposte a indagini.

(60) I sistemi di IA utilizzati nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere hanno effetti su persone che si trovano spesso in una posizione particolarmente vulnerabile e il cui futuro dipende dall'esito delle azioni delle autorità pubbliche competenti. L'accuratezza, la natura non discriminatoria e la trasparenza dei sistemi di IA utilizzati in tali contesti sono pertanto particolarmente importanti per garantire il rispetto dei diritti fondamentali delle persone interessate, in particolare i loro diritti alla libera circolazione, alla non discriminazione, alla protezione della vita privata e dei dati personali, alla protezione internazionale e alla buona amministrazione. È pertanto opportuno classificare come ad alto rischio, nella misura in cui il loro uso è consentito dal pertinente diritto dell'Unione e nazionale, i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, o per loro conto, o dalle istituzioni, dagli organi o dagli organismi dell'Unione, incaricati di compiti in materia di migrazione, asilo e gestione del controllo delle frontiere, come poligrafi e strumenti analoghi, per valutare taluni rischi presentati da persone fisiche che entrano nel territorio di uno Stato membro o presentano domanda di visto o di asilo, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto e di permesso di soggiorno e dei relativi reclami in relazione all'obiettivo di determinare l'ammissibilità delle persone fisiche che richiedono tale status, compresa la connessa valutazione dell'affidabilità degli elementi probatori, al fine di individuare, riconoscere o identificare persone fisiche nel contesto della migrazione, dell'asilo e della gestione del controllo delle frontiere con l'eccezione della verifica dei documenti di viaggio.

I sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere disciplinati dal presente regolamento dovrebbero essere conformi ai pertinenti requisiti procedurali stabiliti dal regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio¹⁴⁸, dalla direttiva 2013/32/UE del Parlamento europeo e del Consiglio,¹⁴⁹ e da altre pertinenti disposizioni di diritto dell'Unione. I sistemi di IA nel settore della migrazione, dell'asilo e della gestione del controllo delle frontiere non dovrebbero in alcun caso essere utilizzati dagli Stati membri o dalle istituzioni, dagli organi o dagli organismi dell'Unione come mezzo per eludere gli obblighi internazionali a essi derivanti a titolo della convenzione delle Nazioni Unite relativa allo status dei rifugiati firmata a Ginevra il 28 luglio 1951, modificata dal protocollo del 31 gennaio 196. Essi non dovrebbero essere utilizzati per violare in alcun modo il principio di non respingimento o per negare sicure ed efficaci vie legali di ingresso nel territorio dell'Unione, compreso il diritto alla protezione internazionale.

¹⁴⁸ Regolamento (CE) n. 810/2009 del Parlamento europeo e del Consiglio, del 13 luglio 2009, che istituisce un Codice comunitario dei visti (codice dei visti) (GU L 243 del 15.9.2009, pag. 1).

¹⁴⁹ Direttiva 2013/32/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, recante procedure comuni ai fini del riconoscimento e della revoca dello status di protezione internazionale (GU L 180 del 29.6.2013, pag. 60).

- (61) Alcuni sistemi di IA destinati all'amministrazione della giustizia e ai processi democratici dovrebbero essere classificati come sistemi ad alto rischio, in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale. È in particolare opportuno, al fine di far fronte ai rischi di potenziali distorsioni, errori e opacità, classificare come ad alto rischio i sistemi di IA destinati a essere utilizzati da un'autorità giudiziaria o per suo conto per assistere le autorità giudiziarie nelle attività di ricerca e interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti. Anche i sistemi di IA destinati a essere utilizzati dagli organismi di risoluzione alternativa delle controversie a tali fini dovrebbero essere considerati ad alto rischio quando gli esiti dei procedimenti di risoluzione alternativa delle controversie producono effetti giuridici per le parti. L'utilizzo di strumenti di IA può fornire sostegno al potere decisionale dei giudici o all'indipendenza del potere giudiziario, ma non dovrebbe sostituirlo: il processo decisionale finale deve rimanere un'attività a guida umana. Non è tuttavia opportuno estendere la classificazione dei sistemi di IA come ad alto rischio ai sistemi di IA destinati ad attività amministrative puramente accessorie, che non incidono sull'effettiva amministrazione della giustizia nei singoli casi, quali l'anonimizzazione o la pseudonimizzazione di decisioni, documenti o dati giudiziari, la comunicazione tra il personale, i compiti amministrativi.

- (62) Fatte salve le norme previste dal regolamento (UE) 2024/... del Parlamento europeo e del Consiglio¹⁵⁰⁺, e al fine di affrontare i rischi di indebite interferenze esterne sul diritto di voto sancito dall'articolo 39 della Carta e di effetti negativi sulla democrazia e sullo Stato di diritto, i sistemi di IA destinati a essere utilizzati per influenzare l'esito di elezioni o referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum dovrebbero essere classificati come sistemi di IA ad alto rischio, ad eccezione dei sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.
- (63) Il fatto che un sistema di IA sia classificato come sistema di IA ad alto rischio a norma del presente regolamento non dovrebbe essere interpretato come un'indicazione del fatto che l'utilizzo del sistema sia lecito a norma di altri atti giuridici dell'Unione o del diritto nazionale compatibile con il diritto dell'Unione, ad esempio in materia di protezione dei dati personali, uso di poligrafi e strumenti analoghi o di altri sistemi atti a rilevare lo stato emotivo delle persone fisiche. Qualsiasi siffatto utilizzo dovrebbe continuare a verificarsi solo in conformità dei requisiti applicabili risultanti dalla Carta e dagli atti applicabili di diritto derivato dell'Unione e di diritto nazionale. Il presente regolamento non dovrebbe essere inteso come un fondamento giuridico per il trattamento dei dati personali, comprese, ove opportuno, categorie particolari di dati personali, salvo quando diversamente disposto in modo specifico dal presente regolamento.

¹⁵⁰ Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del..., relativo alla trasparenza e al targeting della pubblicità politica (GU L, ..., ELI: ...).

⁺ GU: inserire nel testo il numero del regolamento di cui al doc. PE 90/23 (2021/0381(COD)) e completare la corrispondente nota a piè di pagina.

(64) Al fine di attenuare i rischi derivanti dai sistemi di IA ad alto rischio immessi sul mercato o messi in servizio e per garantire un elevato livello di affidabilità, è opportuno applicare determinati requisiti obbligatori ai sistemi di IA ad alto rischio, tenendo conto della finalità prevista e del contesto dell'uso del sistema di IA e conformemente al sistema di gestione dei rischi che deve essere stabilito dal fornitore. Le misure adottate dai fornitori per conformarsi ai requisiti obbligatori del presente regolamento dovrebbero tenere conto dello stato dell'arte generalmente riconosciuto in materia di IA ed essere proporzionate ed efficaci per conseguire gli obiettivi del presente regolamento. Sulla base del nuovo quadro legislativo, come chiarito nella comunicazione della Commissione "La "Guida blu" all'attuazione della normativa UE sui prodotti 2022", di norma più di un atto giuridico della normativa di armonizzazione dell'Unione può essere applicabile a un prodotto, poiché quest'ultimo può essere messo a disposizione o messo in servizio solo se risulta conforme a tutta la normativa di armonizzazione dell'Unione applicabile. I pericoli dei sistemi di IA disciplinati dai requisiti del presente regolamento riguardano aspetti diversi rispetto alla vigente normativa di armonizzazione dell'Unione e pertanto i requisiti del presente regolamento completerebbero il corpus esistente della normativa di armonizzazione dell'Unione. Ad esempio, le macchine o i dispositivi medici in cui è integrato un sistema di IA potrebbero presentare rischi non affrontati dai requisiti essenziali di sicurezza e di tutela della salute stabiliti nella pertinente normativa armonizzata dell'Unione, in quanto tale normativa settoriale non affronta i rischi specifici dei sistemi di IA.

Ciò richiede un'applicazione simultanea e complementare dei vari atti legislativi. Al fine di garantire la coerenza ed evitare oneri amministrativi e costi inutili, i fornitori di un prodotto contenente uno o più sistemi di IA ad alto rischio cui si applicano i requisiti del presente regolamento e della normativa di armonizzazione dell'Unione basata sul nuovo quadro legislativo ed elencata in un allegato del presente regolamento dovrebbero avere flessibilità per quanto riguarda le decisioni operative sulle maniere per garantire in modo ottimale la conformità di un prodotto contenente uno o più sistemi di IA a tutti i requisiti applicabili di tale normativa armonizzata dell'Unione. Tale flessibilità potrebbe significare, ad esempio, che il fornitore decide di integrare una parte dei necessari processi di prova e comunicazione, nonché delle informazioni e della documentazione richieste a norma del presente regolamento nella documentazione e nelle procedure già esistenti richieste dalla vigente normativa di armonizzazione dell'Unione sulla base del nuovo quadro legislativo ed elencate in un allegato del presente regolamento. Ciò non dovrebbe in alcun modo compromettere l'obbligo del fornitore di rispettare tutti i requisiti applicabili.

- (65) Il sistema di gestione dei rischi dovrebbe essere costituito da un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio. Tale processo dovrebbe mirare a individuare e attenuare i rischi pertinenti dei sistemi di IA per la salute, la sicurezza e i diritti fondamentali. Il sistema di gestione dei rischi dovrebbe essere periodicamente riesaminato e aggiornato per garantirne l'efficacia costante, nonché la giustificazione e la documentazione delle eventuali decisioni e azioni significative adottate a norma del presente regolamento. Tale processo dovrebbe garantire che il fornitore individui rischi o impatti negativi e attui misure di attenuazione per i rischi noti e ragionevolmente prevedibili dei sistemi di IA per la salute, la sicurezza e i diritti fondamentali alla luce della loro finalità prevista e del loro uso improprio ragionevolmente prevedibile, compresi gli eventuali rischi derivanti dall'interazione tra il sistema di IA e l'ambiente in cui opera. Il sistema di gestione dei rischi dovrebbe adottare le misure di gestione dei rischi più appropriate alla luce dello stato dell'arte in materia di IA. Nell'individuare le misure di gestione dei rischi più appropriate, il fornitore dovrebbe documentare e spiegare le scelte effettuate e, se del caso, coinvolgere esperti e portatori di interessi esterni. Nell'individuare l'uso improprio ragionevolmente prevedibile dei sistemi di IA ad alto rischio, il fornitore dovrebbe contemplare gli usi di sistemi di IA che, pur non essendo direttamente coperti dalla finalità prevista e considerati nelle istruzioni per l'uso, si può ragionevolmente prevedere derivino da un comportamento umano facilmente prevedibile nel contesto delle caratteristiche e dell'uso specifici di un determinato sistema di IA. Qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità della sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali, dovrebbe essere inclusa nelle istruzioni per l'uso fornite dal fornitore. L'obiettivo è garantire che il deployer sia consapevole e ne tenga conto quando utilizza il sistema di IA ad alto rischio. L'individuazione e l'attuazione di misure di attenuazione dei rischi per un uso improprio prevedibile a norma del presente regolamento non dovrebbero richiedere, da parte del fornitore per farvi fronte, specifiche formazioni aggiuntive per il sistema di IA ad alto rischio. I fornitori sono tuttavia incoraggiati a prendere in considerazione tali misure di formazione aggiuntive per attenuare gli usi impropri ragionevolmente prevedibili, ove necessario e opportuno.

- (66) Tali requisiti dovrebbero applicarsi ai sistemi di IA ad alto rischio per quanto concerne la gestione dei rischi, la qualità e la pertinenza dei set di dati utilizzati, la documentazione tecnica e la conservazione delle registrazioni, la trasparenza e la fornitura di informazioni ai deployer, la sorveglianza umana e la robustezza, l'accuratezza e la cibersecurity. Tali requisiti sono necessari per attenuare efficacemente i rischi per la salute, la sicurezza e i diritti fondamentali e, non essendo ragionevolmente disponibili altre misure meno restrittive degli scambi, non costituiscono limitazioni ingiustificate del commercio.

(67) Dati di alta qualità e l'accesso a dati di alta qualità svolgono un ruolo essenziale nel fornire una struttura e garantire le prestazioni di molti sistemi di IA, in particolare quando si utilizzano tecniche che prevedono l'addestramento di modelli, al fine di garantire che il sistema di IA ad alto rischio funzioni come previsto e in maniera sicura e che non diventi una fonte di discriminazione vietata dal diritto dell'Unione. Per disporre di set di dati di addestramento, convalida e prova di elevata qualità è necessario attuare adeguate pratiche di governance e gestione dei dati. I set di dati di addestramento, convalida e prova, incluse le etichette, dovrebbero essere pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista del sistema. Al fine di agevolare il rispetto del diritto dell'Unione in materia di protezione dei dati, come il regolamento (UE) 2016/679, le pratiche di governance e di gestione dei dati dovrebbero includere, nel caso dei dati personali, la trasparenza in merito alla finalità originaria della raccolta dei dati. I set di dati dovrebbero inoltre possedere le proprietà statistiche appropriate, anche per quanto riguarda le persone o i gruppi di persone in relazione ai quali il sistema di IA ad alto rischio è destinato a essere usato, prestando particolare attenzione all'attenuazione di possibili distorsioni nei set di dati, suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future (feedback loops - "circuiti di feedback"). Le distorsioni possono ad esempio essere intrinseche ai set di dati di base, specie se si utilizzano dati storici, o generate quando i sistemi sono attuati in contesti reali.

I risultati forniti dai sistemi di IA potrebbero essere influenzati da tali distorsioni intrinseche, che sono destinate ad aumentare gradualmente e quindi a perpetuare e amplificare le discriminazioni esistenti, in particolare nei confronti delle persone che appartengono a determinati gruppi vulnerabili, inclusi gruppi razziali o etnici. Il requisito secondo cui i set di dati dovrebbero essere, per quanto possibile, completi ed esenti da errori non dovrebbe incidere sull'uso di tecniche di tutela della vita privata nel contesto dello sviluppo e della prova dei sistemi di IA. In particolare i set di dati dovrebbero tenere conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico contesto geografico, contestuale, comportamentale o funzionale nel quale il sistema di IA ad alto rischio è destinato a essere usato. I requisiti relativi alla governance dei dati possono essere soddisfatti ricorrendo a terzi che offrono servizi di conformità certificati, compresa la verifica della governance dei dati, dell'integrità dei set di dati e delle pratiche di addestramento, convalida e prova dei dati, purché sia garantita la conformità ai requisiti in materia di dati di cui al presente regolamento.

- (68) Ai fini dello sviluppo e della valutazione di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli europei dell'innovazione digitale, gli impianti di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei settori di attività di tali attori soggetti al presente regolamento. Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA. Ad esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di IA a partire da tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata governance istituzionale. Le autorità competenti interessate, comprese quelle settoriali, che forniscono o sostengono l'accesso ai dati, possono anche sostenere la fornitura di dati di alta qualità a fini di addestramento, convalida e prova dei sistemi di IA.
- (69) Il diritto alla vita privata e alla protezione dei dati personali deve essere garantito durante l'intero ciclo di vita del sistema di IA. A tale riguardo, i principi della minimizzazione dei dati e della protezione dei dati fin dalla progettazione e per impostazione predefinita, sanciti dal diritto dell'Unione in materia di protezione dei dati, sono applicabili nel trattamento dei dati personali. Le misure adottate dai fornitori per garantire il rispetto di tali principi possono includere non solo l'anonimizzazione e la cifratura, ma anche l'uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di IA senza trasmissione tra le parti o copia degli stessi dati grezzi o strutturati, fatti salvi i requisiti in materia di governance dei dati di cui al presente regolamento.

- (70) Al fine di proteggere i diritti altrui contro la discriminazione che potrebbe derivare dalla distorsione nei sistemi di IA, è opportuno che i fornitori, in via eccezionale e nella misura strettamente necessaria al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche e previa attuazione di tutte le condizioni applicabili previste dal presente regolamento unitamente alle condizioni previste dai regolamenti (UE) 2016/679 e (UE) 2018/1725 e dalla direttiva (UE) 2016/680, siano in grado di trattare anche categorie particolari di dati personali, come questione di interesse pubblico rilevante ai sensi dell'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679 e dell'articolo 10, paragrafo 2, lettera g), del regolamento (UE) 2018/1725.
- (71) Disporre di informazioni comprensibili sulle modalità di sviluppo dei sistemi di IA ad alto rischio e sulle loro modalità di funzionamento durante tutto il ciclo di vita è essenziale per consentire la tracciabilità di tali sistemi, verificare la conformità ai requisiti di cui al presente regolamento, monitorarne il funzionamento e svolgere il monitoraggio successivo all'immissione sul mercato. Occorre a tal fine conservare le registrazioni e disporre di una documentazione tecnica contenente le informazioni necessarie per valutare la conformità del sistema di IA ai requisiti pertinenti e agevolare il monitoraggio successivo all'immissione sul mercato. Tali informazioni dovrebbero includere le caratteristiche, le capacità e i limiti generali del sistema, gli algoritmi, i dati, l'addestramento, i processi di prova e di convalida utilizzati, nonché la documentazione sul pertinente sistema di gestione dei rischi redatta in forma chiara e comprensibile. È opportuno tenere aggiornata in modo adeguato la documentazione tecnica durante l'intero ciclo di vita del sistema di IA. Inoltre, i sistemi di IA ad alto rischio dovrebbero consentire, a livello tecnico, la registrazione automatica degli eventi, mediante "log", per la durata del ciclo di vita del sistema.

- (72) Per rispondere alle preoccupazioni relative all'opacità e alla complessità di determinati sistemi di IA e aiutare i deployer ad adempiere ai loro obblighi a norma del presente regolamento, è opportuno imporre la trasparenza per i sistemi di IA ad alto rischio prima che siano immessi sul mercato o messi in servizio. I sistemi di IA ad alto rischio dovrebbero essere progettati in modo da consentire ai deployer di comprendere il funzionamento del sistema di IA, valutarne la funzionalità e comprenderne i punti di forza e i limiti. I sistemi di IA ad alto rischio dovrebbero essere accompagnati da informazioni adeguate sotto forma di istruzioni per l'uso. Tali informazioni dovrebbero includere le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA. Tali elementi comprenderebbero informazioni su possibili circostanze note e prevedibili connesse all'uso del sistema di IA ad alto rischio, compresa l'azione del deployer suscettibile di influenzare il comportamento e le prestazioni del sistema, nel quadro dei quali il sistema di IA può comportare rischi per la salute, la sicurezza e i diritti fondamentali, sulle modifiche che sono state predeterminate e valutate a fini di conformità dal fornitore e sulle pertinenti misure di sorveglianza umana, comprese le misure volte a facilitare l'interpretazione degli output del sistema di IA da parte dei deployer. La trasparenza, comprese le istruzioni per l'uso che la accompagnano, dovrebbe aiutare i deployer a utilizzare il sistema e a prendere decisioni informate. Tra l'altro, i deployer dovrebbero essere nella posizione migliore per effettuare la scelta corretta del sistema che intendono utilizzare alla luce degli obblighi loro applicabili, essere a conoscenza degli usi previsti e vietati e utilizzare il sistema di IA in modo corretto e opportuno. Al fine di migliorare la leggibilità e l'accessibilità delle informazioni incluse nelle istruzioni per l'uso, se del caso, dovrebbero essere inclusi, esempi illustrativi, ad esempio sulle limitazioni e sugli usi previsti e vietati del sistema di IA. I fornitori dovrebbero garantire che tutta la documentazione, comprese le istruzioni per l'uso, contenga informazioni significative, complete, accessibili e comprensibili, tenendo conto delle esigenze e delle conoscenze prevedibili dei deployer destinatari. Le istruzioni per l'uso dovrebbero essere messe a disposizione in una lingua che possa essere compresa facilmente dai deployer destinatari, secondo quanto stabilito dallo Stato membro interessato.

(73) I sistemi di IA ad alto rischio dovrebbero essere progettati e sviluppati in modo da consentire alle persone fisiche di sorvegliarne il funzionamento, garantire che siano utilizzati come previsto e che i loro impatti siano affrontati durante il ciclo di vita del sistema. Il fornitore del sistema dovrebbe a tal fine individuare misure di sorveglianza umana adeguate prima dell'immissione del sistema sul mercato o della sua messa in servizio. Tali misure dovrebbero in particolare garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo. È inoltre essenziale, se del caso, garantire che i sistemi di IA ad alto rischio includano meccanismi per guidare e informare la persona fisica alla quale è stata affidata la sorveglianza umana affinché prenda decisioni informate in merito alla possibilità, ai tempi e alle modalità di intervento, onde evitare conseguenze negative o rischi, oppure affinché arresti il sistema, qualora non funzionasse come previsto. Tenuto conto delle conseguenze significative per le persone in caso di una corrispondenza non corretta da parte di determinati sistemi di identificazione biometrica, è opportuno prevedere un requisito rafforzato di sorveglianza umana per tali sistemi, in modo che il deployer non possa adottare alcuna azione o decisione sulla base dell'identificazione risultante dal sistema, a meno che ciò non sia stato verificato e confermato separatamente da almeno due persone fisiche. Tali persone potrebbero provenire da una o più entità e comprendere la persona che gestisce o utilizza il sistema. Tale requisito non dovrebbe comportare oneri o ritardi inutili e potrebbe essere sufficiente che le verifiche separate da parte delle diverse persone siano automaticamente registrate nei log generati dal sistema. Date le specificità dei settori delle attività di contrasto, della migrazione, del controllo delle frontiere e dell'asilo, tale requisito non dovrebbe applicarsi se il diritto dell'Unione o nazionale ritenga sproporzionata la sua applicazione.

- (74) Le prestazioni dei sistemi di IA ad alto rischio dovrebbero essere coerenti durante tutto il loro ciclo di vita e tali sistemi dovrebbero garantire un livello adeguato di accuratezza, robustezza e cbersicurezza, alla luce della loro finalità prevista e conformemente allo stato dell'arte generalmente riconosciuto. La Commissione e le organizzazioni e i portatori di interessi pertinenti sono incoraggiati a tenere in debita considerazione l'attenuazione dei rischi e degli impatti negativi del sistema di IA. Il livello atteso delle metriche di prestazione dovrebbe essere dichiarato nelle istruzioni per l'uso che accompagnano il sistema. I fornitori sono invitati a comunicare tali informazioni ai deployer in modo chiaro e facilmente comprensibile, senza malintesi o affermazioni fuorvianti. Il diritto dell'Unione in materia di metrologia legale, comprese le direttive 2014/31/UE¹⁵¹ e 2014/32/UE¹⁵² del Parlamento europeo e del Consiglio, mira a garantire l'accuratezza delle misurazioni e a favorire la trasparenza e l'equità delle transazioni commerciali. In tale contesto, in cooperazione con i portatori di interessi e le organizzazioni pertinenti, quali le autorità di metrologia e di analisi comparativa, la Commissione dovrebbe incoraggiare, se del caso, lo sviluppo di parametri di riferimento e metodologie di misurazione per i sistemi di IA. A tal fine, la Commissione dovrebbe prendere atto dei partner internazionali che operano nel settore della metrologia, collaborando con essi, e dei pertinenti indicatori di misurazione relativi all'IA.

¹⁵¹ Direttiva 2014/31/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di strumenti per pesare a funzionamento non automatico (GU L 96 del 29.3.2014, pag. 107).

¹⁵² Direttiva 2014/32/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di strumenti di misura (GU L 096 del 29.3.2014, pag. 149).

- (75) La robustezza tecnica è un requisito fondamentale dei sistemi di IA ad alto rischio. Essi dovrebbero essere resilienti in relazione a comportamenti dannosi o altrimenti indesiderati che possono derivare da limitazioni all'interno dei sistemi o dell'ambiente in cui i sistemi funzionano (ad esempio errori, guasti, incongruenze, situazioni impreviste). È pertanto opportuno adottare misure tecniche e organizzative per garantire la robustezza dei sistemi di IA ad alto rischio, ad esempio progettando e sviluppando soluzioni tecniche adeguate per prevenire o ridurre al minimo i comportamenti dannosi o altrimenti indesiderati. Tali soluzioni tecniche possono comprendere, ad esempio, meccanismi che consentano al sistema di interrompere in modo sicuro il proprio funzionamento (piani fail-safe) in presenza di determinate anomalie o quando il funzionamento ha luogo al di fuori di determinati limiti prestabiliti. La mancata protezione da tali rischi potrebbe avere ripercussioni sulla sicurezza o incidere negativamente sui diritti fondamentali, ad esempio a causa di decisioni errate o di output sbagliati o distorti generati dal sistema di IA.
- (76) La cibersecurity svolge un ruolo cruciale nel garantire che i sistemi di IA siano resilienti ai tentativi compiuti da terzi con intenzioni malevole che, sfruttando le vulnerabilità del sistema, mirano ad alterarne l'uso, il comportamento, le prestazioni o a comprometterne le proprietà di sicurezza. Gli attacchi informatici contro i sistemi di IA possono far leva sulle risorse specifiche dell'IA, quali i set di dati di addestramento (ad esempio il data poisoning, "avvelenamento dei dati") o i modelli addestrati (ad esempio gli adversarial attacks, "attacchi antagonisti" o la membership inference, "attacchi inferenziali"), o sfruttare le vulnerabilità delle risorse digitali del sistema di IA o dell'infrastruttura TIC sottostante. Al fine di garantire un livello di cibersecurity adeguato ai rischi, è pertanto opportuno che i fornitori di sistemi di IA ad alto rischio adottino misure adeguate, come controlli di sicurezza, anche tenendo debitamente conto dell'infrastruttura TIC sottostante.

(77) Fatti salvi i requisiti relativi alla robustezza e all'accuratezza di cui al presente regolamento, i sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali, ai sensi di tale regolamento possono dimostrare la conformità ai requisiti di cibersecurity del presente regolamento rispettando i requisiti essenziali di cibersecurity a norma di tale regolamento. Quando rispettano i requisiti essenziali del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali, i sistemi di IA ad alto rischio dovrebbero essere considerati conformi ai requisiti di cibersecurity di cui al presente regolamento nella misura in cui il rispetto di tali requisiti sia dimostrato nella dichiarazione di conformità UE, o in parti di essa, rilasciata a norma di tale regolamento. A tal fine, la valutazione dei rischi di cibersecurity, associati a un prodotto con elementi digitali classificati come sistemi di IA ad alto rischio ai sensi del presente regolamento, effettuata a norma del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali, dovrebbe tenere in considerazione i rischi per la cyberresilienza di un sistema di IA per quanto riguarda i tentativi di terzi non autorizzati di modificarne l'uso, il comportamento o le prestazioni, comprese le vulnerabilità specifiche dell'IA, quali il data poisoning ("avvelenamento dei dati") o gli adversarial attack ("attacchi antagonisti"), nonché, se del caso, i rischi per i diritti fondamentali come disposto dal presente regolamento.

(78) La procedura di valutazione della conformità di cui al presente regolamento dovrebbe applicarsi in relazione ai requisiti essenziali di cibersicurezza di un prodotto con elementi digitali disciplinato dal regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e classificato come sistema di IA ad alto rischio a norma del presente regolamento. Tuttavia, tale norma non dovrebbe comportare una riduzione del livello di garanzia necessario per i prodotti con elementi digitali critici disciplinati dal regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali. Pertanto, in deroga a detta norma, i sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento e che sono anche qualificati come prodotti con elementi digitali importanti e critici a norma del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali, e ai quali si applica la procedura di valutazione della conformità basata sul controllo interno in allegato al presente regolamento, sono soggetti alle disposizioni in materia di valutazione della conformità del regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali per quanto riguarda i requisiti essenziali di cibersicurezza di tale regolamento. In tal caso, per tutti gli altri aspetti disciplinati dal presente regolamento dovrebbero applicarsi le rispettive disposizioni in materia di valutazione della conformità basata sul controllo interno, in allegato al presente regolamento. Sulla base delle conoscenze e delle competenze dell'ENISA in merito alla politica in materia di cibersicurezza e ai relativi compiti assegnati all'ENISA a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio¹⁵³, la Commissione dovrebbe cooperare con l'ENISA sulle questioni relative alla cibersicurezza dei sistemi di IA.

¹⁵³ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

- (79) È opportuno che una specifica persona fisica o giuridica, definita come il fornitore, si assuma la responsabilità dell'immissione sul mercato o della messa in servizio di un sistema di IA ad alto rischio, a prescindere dal fatto che tale persona fisica o giuridica sia la persona che ha progettato o sviluppato il sistema.
- (80) In qualità di firmatari della Convenzione delle Nazioni Unite sui diritti delle persone con disabilità, l'Unione e gli Stati membri sono tenuti, dal punto di vista giuridico, a proteggere le persone con disabilità dalla discriminazione e a promuoverne l'uguaglianza, a garantire che le persone con disabilità abbiano accesso, su un piano di parità con gli altri, alle tecnologie e ai sistemi di informazione e comunicazione e a garantire il rispetto della vita privata delle persone con disabilità. In considerazione dell'importanza e dell'utilizzo crescenti dei sistemi di IA, l'applicazione dei principi della progettazione universale a tutti i nuovi servizi e tecnologie dovrebbe garantire un accesso pieno e paritario a tutti coloro che sono potenzialmente interessati dalle tecnologie di IA o che le utilizzano, ivi comprese le persone con disabilità, in modo da tenere pienamente conto delle loro dignità e diversità intrinseche. È pertanto essenziale che i fornitori garantiscano la piena conformità ai requisiti di accessibilità, anche alla direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio¹⁵⁴ e alla direttiva (UE) 2019/882. I fornitori dovrebbero garantire il rispetto di tali requisiti fin dalla progettazione. Pertanto, le misure necessarie dovrebbero essere quanto più possibile integrate nella progettazione dei sistemi di IA ad alto rischio.

¹⁵⁴ Direttiva (UE) 2016/2102 del Parlamento europeo e del Consiglio, del 26 ottobre 2016, relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici (GU L 327 del 2.12.2016, pag. 1).

- (81) È opportuno che il fornitore istituisca un solido sistema di gestione della qualità, garantisca l'espletamento della procedura di valutazione della conformità richiesta, rediga la documentazione pertinente e istituisca un sistema robusto per il monitoraggio successivo all'immissione sul mercato. I fornitori di sistemi di IA ad alto rischio che sono soggetti a obblighi relativi ai sistemi di gestione della qualità conformemente al pertinente diritto settoriale dell'Unione dovrebbero avere la possibilità di includere gli elementi del sistema di gestione della qualità di cui al presente regolamento nell'ambito del sistema di gestione della qualità esistente previsto da tale altro diritto settoriale dell'Unione. La complementarità tra il presente regolamento e il diritto settoriale vigente dell'Unione dovrebbe essere tenuta in considerazione anche nelle future attività di normazione o negli orientamenti adottati dalla Commissione. Le autorità pubbliche che mettono in servizio sistemi di IA ad alto rischio per uso proprio possono adottare e attuare le regole per il sistema di gestione della qualità nell'ambito del sistema di gestione della qualità adottato a livello nazionale o regionale, a seconda dei casi, tenendo conto delle specificità del settore come pure delle competenze e dell'organizzazione dell'autorità pubblica interessata.

- (82) Al fine di consentire l'applicazione del presente regolamento e di creare condizioni di parità per gli operatori, e tenendo conto delle diverse forme di messa a disposizione di prodotti digitali, è importante garantire che, in qualsiasi circostanza, una persona stabilita nell'Unione possa fornire alle autorità tutte le informazioni necessarie sulla conformità di un sistema di IA. Pertanto, prima di mettere a disposizione i propri sistemi di IA nell'Unione, i fornitori stabiliti in paesi terzi dovrebbero nominare, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione. Tale rappresentante autorizzato svolge un ruolo chiave nel garantire la conformità dei sistemi di IA ad alto rischio immessi sul mercato o messi in servizio nell'Unione da tali fornitori non stabiliti nell'Unione e nel servire da loro referente stabilito nell'Unione.
- (83) Alla luce della natura e della complessità della catena del valore per i sistemi di IA e in linea con il nuovo quadro legislativo, è essenziale garantire la certezza del diritto e facilitare il rispetto del presente regolamento. È pertanto necessario chiarire il ruolo e gli obblighi specifici degli operatori pertinenti lungo tale catena del valore, come importatori e distributori che possono contribuire allo sviluppo dei sistemi di IA. In determinate situazioni tali operatori potrebbero agire contemporaneamente in più di un ruolo e dovrebbero pertanto adempiere cumulativamente tutti gli obblighi pertinenti associati a tali ruoli. Ad esempio, un operatore potrebbe agire contemporaneamente come distributore e importatore.

- (84) Al fine di garantire la certezza del diritto, è necessario chiarire che, a determinate condizioni specifiche, qualsiasi distributore, importatore, deployer o altro terzo dovrebbe essere considerato un fornitore di un sistema di IA ad alto rischio e, pertanto, assumere tutti gli obblighi del caso. Ciò si verifica ove tale parte apponga il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi. Ciò si verifica anche ove tale parte apporti una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio e in modo che resti un sistema di IA ad alto rischio a norma del presente regolamento, ovvero ove modifichi la finalità prevista di un sistema di IA, compreso un sistema di IA per finalità generali, che non è stato classificato come sistema ad alto rischio ed è già immesso sul mercato o messo in servizio, in modo tale da rendere il sistema di IA un sistema di IA ad alto rischio a norma del presente regolamento. Tali disposizioni dovrebbero applicarsi fatte salve le disposizioni più specifiche stabilite in alcune normative di armonizzazione dell'Unione basate sul nuovo quadro legislativo, unitamente al quale dovrebbe applicarsi il presente regolamento. Ad esempio, l'articolo 16, paragrafo 2, del regolamento (UE) 2017/745, che stabilisce che talune modifiche non dovrebbero essere considerate modifiche di un dispositivo tali da compromettere la sua conformità alle prescrizioni applicabili, dovrebbe continuare ad applicarsi ai sistemi di IA ad alto rischio che sono dispositivi medici ai sensi di tale regolamento.

- (85) I sistemi di IA per finalità generali possono essere utilizzati da soli come sistemi di IA ad alto rischio o essere componenti di altri sistemi di IA ad alto rischio. Pertanto, data la loro natura particolare e al fine di garantire un'equa ripartizione delle responsabilità lungo la catena del valore dell'IA, i fornitori di tali sistemi, indipendentemente dal fatto che questi possano essere utilizzati di per sé come sistemi di IA ad alto rischio da altri fornitori o come componenti di sistemi di IA ad alto rischio, e salvo se diversamente disposto dal presente regolamento, dovrebbero cooperare strettamente con i fornitori dei pertinenti sistemi di IA ad alto rischio per consentire loro di conformarsi ai pertinenti obblighi previsti dal presente regolamento e con le autorità competenti istituite a norma del presente regolamento.
- (86) Qualora, alle condizioni di cui al presente regolamento, il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA non dovesse più essere considerato il fornitore ai fini del presente regolamento, e se tale fornitore non ha espressamente escluso la modifica del sistema di IA in un sistema di IA ad alto rischio, il precedente fornitore dovrebbe comunque cooperare strettamente e mettere a disposizione le informazioni necessarie nonché fornire l'accesso tecnico ragionevolmente atteso e qualsiasi altra forma di assistenza che sono richiesti per l'adempimento degli obblighi di cui al presente regolamento, in particolare per quanto riguarda la conformità alla valutazione della conformità dei sistemi di IA ad alto rischio.
- (87) Inoltre, se un sistema di IA ad alto rischio che è un componente di sicurezza di un prodotto rientrante nell'ambito di applicazione della normativa di armonizzazione dell'Unione basata sul nuovo quadro legislativo non è immesso sul mercato o messo in servizio separatamente dal prodotto, il fabbricante del prodotto quale definito in tale normativa dovrebbe adempiere gli obblighi del fornitore stabiliti nel presente regolamento e, in particolare, dovrebbe garantire che il sistema di IA integrato nel prodotto finale soddisfa i requisiti del presente regolamento.

- (88) Lungo la catena del valore dell'IA, spesso più parti forniscono sistemi di IA, strumenti e servizi, ma anche componenti o processi, che sono integrati dal fornitore nel sistema di IA con varie finalità, inclusi l'addestramento dei modelli, la riqualificazione dei modelli, la prova e la valutazione dei modelli, l'integrazione nel software o altri aspetti dello sviluppo dei modelli. Tali parti svolgono un ruolo importante nella catena del valore nei confronti del fornitore del sistema di IA ad alto rischio in cui i loro sistemi di IA, strumenti, servizi, componenti o processi sono integrati e dovrebbero fornire a tale fornitore mediante accordo scritto le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari sulla base dello stato dell'arte generalmente riconosciuto, al fine di consentire al fornitore di adempiere pienamente gli obblighi di cui al presente regolamento, senza compromettere i propri diritti di proprietà intellettuale o segreti commerciali.
- (89) I terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti di IA diversi dai modelli di IA per finalità generali non dovrebbero essere tenuti a conformarsi a requisiti relativi alle responsabilità lungo la catena del valore dell'IA, in particolare nei confronti del fornitore che li ha utilizzati o integrati, quando tali strumenti, servizi, processi o componenti di IA sono resi accessibili con licenza libera e open source. Gli sviluppatori di strumenti, servizi, processi o componenti di IA liberi e open source diversi dai modelli di IA per finalità generali dovrebbero essere incoraggiati ad attuare pratiche di documentazione ampiamente adottate, come schede di modelli e schede dati, al fine di accelerare la condivisione delle informazioni lungo la catena del valore dell'IA, consentendo la promozione di sistemi di IA affidabili nell'Unione.

- (90) La Commissione potrebbe elaborare e raccomandare clausole contrattuali tipo volontarie tra i fornitori di sistemi di IA ad alto rischio e i terzi che forniscono strumenti, servizi, componenti o processi utilizzati o integrati in sistemi di IA ad alto rischio, al fine di agevolare la cooperazione lungo la catena del valore. Nell'elaborare clausole contrattuali tipo volontarie, la Commissione dovrebbe altresì tenere conto dei possibili requisiti contrattuali applicabili in determinati settori o casi commerciali.
- (91) In considerazione della natura dei sistemi di IA e dei possibili rischi per la sicurezza e i diritti fondamentali associati al loro utilizzo, anche per quanto riguarda la necessità di garantire un adeguato monitoraggio delle prestazioni di un sistema di IA in un contesto reale, è opportuno stabilire responsabilità specifiche per i deployer. È in particolare opportuno che i deployer adottino misure tecniche e organizzative adeguate per garantire di utilizzare i sistemi di IA ad alto rischio conformemente alle istruzioni per l'uso e che siano previsti alcuni altri obblighi in materia di monitoraggio del funzionamento dei sistemi di IA e conservazione delle registrazioni, a seconda dei casi. Inoltre, i deployer dovrebbero garantire che le persone alle quali è affidata l'attuazione delle istruzioni per l'uso e della sorveglianza umana di cui al presente regolamento dispongano delle competenze necessarie, in particolare un livello adeguato di alfabetizzazione, formazione e autorità in materia di IA per svolgere adeguatamente tali compiti. Tali obblighi dovrebbero lasciare impregiudicati altri obblighi dei deployer in relazione ai sistemi di IA ad alto rischio previsti dal diritto dell'Unione o nazionale.

(92) Il presente regolamento lascia impregiudicati gli obblighi dei datori di lavoro di informare o di informare e consultare i lavoratori o i loro rappresentanti a norma del diritto e delle prassi dell'Unione o nazionali, compresa la direttiva 2002/14/CE del Parlamento europeo e del Consiglio¹⁵⁵, in merito alle decisioni di mettere in servizio o utilizzare sistemi di IA. Rimane necessario garantire che i lavoratori e i loro rappresentanti siano informati in merito alla diffusione programmata dei sistemi di IA ad alto rischio sul luogo di lavoro, qualora non siano soddisfatte le condizioni per tali obblighi di informazione o di informazione e consultazione previsti da altri strumenti giuridici. Inoltre, tale diritto di informazione è accessorio e necessario rispetto all'obiettivo di tutelare i diritti fondamentali alla base del presente regolamento. È pertanto opportuno prevedere nel presente regolamento un obbligo di informazione con tale finalità, lasciando impregiudicati i diritti esistenti dei lavoratori.

¹⁵⁵ Direttiva 2002/14/CE del Parlamento europeo e del Consiglio, dell'11 marzo 2002, che istituisce un quadro generale relativo all'informazione e alla consultazione dei lavoratori — (GU L 80 del 23.3.2002, pag. 29).

(93) Se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche dal modo in cui tali sistemi di IA sono utilizzati. I deployer di sistemi di IA ad alto rischio svolgono pertanto un ruolo fondamentale nel garantire la tutela dei diritti fondamentali, integrando gli obblighi del fornitore nello sviluppo del sistema di IA. I deployer sono nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili. I deployer dei sistemi di IA ad alto rischio elencati in un allegato del presente regolamento svolgono inoltre un ruolo cruciale per informare le persone fisiche e, quando adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche, dovrebbero informare, se del caso, queste ultime che sono soggette all'uso del sistema di IA ad alto rischio. Tale informazione dovrebbe includere la finalità prevista e il tipo di decisioni adottate. Il deployer dovrebbe informare inoltre le persone fisiche del loro diritto a una spiegazione previsto dal presente regolamento. Per quanto riguarda i sistemi di IA ad alto rischio utilizzati a fini di attività di contrasto, tale obbligo dovrebbe essere attuato conformemente all'articolo 13 della direttiva (UE) 2016/680.

- (94) Qualsiasi trattamento di dati biometrici interessati dall'uso di sistemi di IA a fini di identificazione biometrica a scopo di contrasto deve essere conforme all'articolo 10 della direttiva (UE) 2016/680, che consente tale trattamento solo se strettamente necessario, fatte salve le tutele adeguate per i diritti e le libertà dell'interessato, e se autorizzato dal diritto dell'Unione o degli Stati membri. Tale uso, se autorizzato, deve inoltre rispettare i principi di cui all'articolo 4, paragrafo 1, della direttiva (UE) 2016/680, tra cui liceità, correttezza e trasparenza, determinazione delle finalità, esattezza e limitazione della conservazione.
- (95) Fatto salvo il diritto dell'Unione applicabile, in particolare il regolamento (UE) 2016/679 e la direttiva (UE) 2016/680, tenendo in considerazione la natura invasiva dei sistemi di identificazione biometrica remota a posteriori, l'uso di tali sistemi dovrebbe essere soggetto a tutele. I sistemi di identificazione biometrica remota a posteriori dovrebbero sempre essere utilizzati in modo proporzionato, legittimo e strettamente necessario e quindi mirato, per quanto riguarda le persone da identificare, il luogo e l'ambito temporale e sulla base di un set di dati chiuso di filmati acquisiti legalmente. In ogni caso, i sistemi di identificazione biometrica remota a posteriori non dovrebbero essere utilizzati nel quadro delle attività di contrasto per condurre una sorveglianza indiscriminata. Le condizioni per l'identificazione biometrica remota a posteriori non dovrebbero, in ogni caso, fornire una base per eludere le condizioni del divieto e le rigorose eccezioni per l'identificazione biometrica remota "in tempo reale".

- (96) Al fine di garantire in modo efficiente la tutela dei diritti fondamentali, i deployer di sistemi di IA ad alto rischio che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici e deployer di taluni sistemi di IA ad alto rischio elencati nell'allegato del presente regolamento, come i soggetti bancari o assicurativi, dovrebbero svolgere una valutazione d'impatto sui diritti fondamentali prima di metterli in uso. I servizi importanti di natura pubblica per le persone possono essere forniti anche da soggetti privati. Gli enti privati che forniscono tali servizi pubblici sono legati a compiti di interesse pubblico, ad esempio nei settori dell'istruzione, dell'assistenza sanitaria, dei servizi sociali, degli alloggi e dell'amministrazione della giustizia. L'obiettivo della valutazione d'impatto sui diritti fondamentali è consentire al deployer di individuare i rischi specifici per i diritti delle persone o dei gruppi di persone che potrebbero essere interessati e di individuare le misure da adottare al concretizzarsi di tali rischi. La valutazione d'impatto dovrebbe essere svolta prima del primo impiego del sistema di IA ad alto rischio e dovrebbe essere aggiornata quando il deployer ritiene che uno qualsiasi dei fattori pertinenti sia cambiato. La valutazione d'impatto dovrebbe individuare i processi pertinenti del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista e dovrebbe includere una descrizione del periodo di tempo in cui il sistema è destinato a essere usato e della relativa frequenza, nonché delle categorie specifiche di persone fisiche e gruppi che potrebbero essere interessati nel contesto specifico di utilizzo.

La valutazione dovrebbe altresì comprendere l'individuazione di rischi specifici di danno che possono incidere sui diritti fondamentali di tali persone o gruppi. Nell'effettuare tale valutazione, il deployer dovrebbe tenere conto delle informazioni pertinenti per un'adeguata valutazione dell'impatto, comprese, tra l'altro, le informazioni trasmesse dal fornitore del sistema di IA ad alto rischio nelle istruzioni per l'uso. Alla luce dei rischi individuati, i deployer dovrebbero stabilire le misure da adottare al concretizzarsi di tali rischi, compresi, ad esempio, i meccanismi di governance in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana secondo le istruzioni per l'uso, o le procedure di gestione dei reclami e di ricorso, dato che potrebbero essere determinanti nell'attenuare i rischi per i diritti fondamentali in casi d'uso concreti. Dopo aver effettuato tale valutazione d'impatto, il deployer dovrebbe darne notifica alla pertinente autorità di vigilanza del mercato. Se del caso, per raccogliere le informazioni pertinenti necessarie a effettuare la valutazione d'impatto, i deployer di sistemi di IA ad alto rischio, in particolare quando i sistemi di IA sono utilizzati nel settore pubblico, potrebbero coinvolgere i portatori di interessi pertinenti, compresi i rappresentanti di gruppi di persone che potrebbero essere interessati dal sistema di IA, gli esperti indipendenti e le organizzazioni della società civile nello svolgimento di tali valutazioni d'impatto e nella progettazione delle misure da adottare al concretizzarsi dei rischi. L'ufficio europeo per l'IA ("ufficio per l'IA") dovrebbe elaborare un modello di questionario al fine di agevolare la conformità e ridurre gli oneri amministrativi per i deployer.

- (97) La nozione di modelli di IA per finalità generali dovrebbe essere chiaramente definita e distinta dalla nozione di sistemi di IA per consentire la certezza del diritto. La definizione dovrebbe basarsi sulle principali caratteristiche funzionali di un modello di IA per finalità generali, in particolare la generalità e la capacità di svolgere con competenza un'ampia gamma di compiti distinti. Questi modelli sono solitamente addestrati su grandi quantità di dati con diversi metodi, come l'apprendimento autosupervisionato, non supervisionato o per rinforzo. I modelli di IA per finalità generali possono essere immessi sul mercato in vari modi, tra cui biblioteche, interfacce di programmazione delle applicazioni (API), download diretto o copia fisica. Tali modelli possono essere ulteriormente modificati o perfezionati con nuovi modelli. Sebbene i modelli di IA siano componenti essenziali dei sistemi di IA, essi non costituiscono di per sé sistemi di IA. I modelli di IA necessitano dell'aggiunta di altri componenti, ad esempio un'interfaccia utente, per diventare sistemi di IA. I modelli di IA sono generalmente integrati nei sistemi di IA e ne fanno parte. Il presente regolamento stabilisce norme specifiche per i modelli di IA per finalità generali e per i modelli di IA per finalità generali che presentano rischi sistemici, le quali dovrebbero applicarsi anche quando tali modelli sono integrati o fanno parte di un sistema di IA. Resta inteso che gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero applicarsi una volta che i modelli di IA per finalità generali sono immessi sul mercato.

Quando il fornitore di un modello di IA per finalità generali integra un modello proprio nel suo sistema di IA messo a disposizione sul mercato o messo in servizio, tale modello dovrebbe essere considerato immesso sul mercato e, pertanto, gli obblighi di cui al presente regolamento per i modelli dovrebbero continuare ad applicarsi in aggiunta a quelli per i sistemi di IA. Gli obblighi previsti per i modelli non dovrebbero in ogni caso applicarsi quando un modello proprio è utilizzato per processi puramente interni che non sono essenziali per fornire un prodotto o un servizio a terzi e i diritti delle persone fisiche restano impregiudicati. Considerati i loro potenziali effetti negativi significativi, i modelli di IA per finalità generali con rischio sistemico dovrebbero sempre essere soggetti ai pertinenti obblighi a norma del presente regolamento. La definizione non dovrebbe includere i modelli di IA utilizzati prima della loro immissione sul mercato solo a scopo di ricerca, sviluppo e prototipazione. Ciò non pregiudica l'obbligo di conformarsi al presente regolamento quando, in seguito a tali attività, un modello è immesso sul mercato.

- (98) Mentre la generalità di un modello potrebbe, tra gli altri criteri, essere determinata anche da una serie di parametri, i modelli con almeno un miliardo di parametri e addestrati con grandi quantità di dati utilizzando l'autosupervisione su larga scala dovrebbero ritenersi caratterizzati da una generalità significativa e in grado di svolgere con competenza un'ampia gamma di compiti distinti.
- (99) I grandi modelli di IA generativi sono un tipico esempio di modello di IA per finalità generali, dato che consentono una generazione flessibile di contenuti, ad esempio sotto forma di testo, audio, immagini o video, che possono prontamente rispondere a un'ampia gamma di compiti distinti.

- (100) Quando un modello di IA per finalità generali è integrato in un sistema di IA o ne fa parte, tale sistema dovrebbe essere considerato un sistema di IA per finalità generali qualora, a causa di tale integrazione, il sistema abbia la capacità di perseguire varie finalità. Un sistema di IA per finalità generali può essere utilizzato direttamente o può essere integrato in altri sistemi di IA.
- (101) I fornitori di modelli di IA per finalità generali hanno un ruolo e una responsabilità particolari lungo la catena del valore dell'IA, poiché i modelli che forniscono possono costituire la base per una serie di sistemi a valle, spesso forniti da fornitori a valle che richiedono una buona comprensione dei modelli e delle loro capacità, sia per consentire l'integrazione di tali modelli nei loro prodotti, sia per adempiere i rispettivi obblighi a norma del presente regolamento o di altri regolamenti. È pertanto opportuno prevedere misure di trasparenza proporzionate, tra cui la redazione e l'aggiornamento della documentazione e la fornitura di informazioni sul modello di IA per finalità generali ai fini del suo utilizzo da parte dei fornitori a valle. La documentazione tecnica dovrebbe essere preparata e tenuta aggiornata dal fornitore del modello di IA per finalità generali allo scopo di metterla a disposizione, su richiesta, dell'ufficio per l'IA e delle autorità nazionali competenti. La serie minima di elementi da includere in tale documentazione dovrebbe essere stabilita in specifici allegati del presente regolamento. Alla Commissione dovrebbe essere conferito il potere di modificare tali allegati mediante atti delegati alla luce degli sviluppi tecnologici in evoluzione.

- (102) I software e i dati, compresi i modelli, rilasciati con licenza libera e open source che consentano loro di essere condivisi apertamente e che gli utenti possano liberamente consultare, utilizzare, modificare e ridistribuire, comprese le loro versioni modificate, possono contribuire alla ricerca e all'innovazione nel mercato e possono offrire notevoli opportunità di crescita per l'economia dell'Unione. I modelli di IA per finalità generali rilasciati con licenza libera e open source dovrebbero essere presi in considerazione per garantire elevati livelli di trasparenza e apertura, se i loro parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici. La licenza dovrebbe essere considerata libera e open source anche quando consente agli utenti di eseguire, copiare, distribuire, studiare, modificare e migliorare i software e i dati, compresi i modelli, purché il modello sia attribuito al fornitore originario e siano rispettate condizioni di distribuzione identiche o comparabili.
- (103) I componenti di IA liberi e open source comprendono i software e i dati, compresi i modelli e i modelli di IA per finalità generali, gli strumenti, i servizi o i processi di un sistema di IA. I componenti di IA liberi e open source possono essere forniti attraverso diversi canali e possono inoltre essere sviluppati su archivi aperti. Ai fini del presente regolamento, i componenti di IA forniti a pagamento o altrimenti monetizzati, anche tramite la fornitura di assistenza tecnica o altri servizi, ad esempio attraverso una piattaforma software, in relazione al componente di IA, o l'utilizzo di dati personali per motivi diversi dal solo miglioramento della sicurezza, della compatibilità o dell'interoperabilità del software, ad eccezione delle transazioni tra microimprese, non dovrebbero beneficiare delle eccezioni previste per i componenti di IA liberi e open source. La messa a disposizione di componenti di IA tramite archivi aperti non dovrebbe, di per sé, costituire monetizzazione.

(104) I fornitori di modelli di IA per finalità generali che sono rilasciati con licenza libera e open source e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono messi pubblicamente a disposizione dovrebbero essere soggetti ad eccezioni per quanto riguarda i requisiti relativi alla trasparenza imposti ai modelli di IA per finalità generali, a meno che non si possa ritenere che presentino un rischio sistemico, nel qual caso la circostanza che il modello sia trasparente e corredato di una licenza open source non dovrebbe ritenersi un motivo sufficiente per escludere la conformità agli obblighi di cui al presente regolamento. In ogni caso, dato che il rilascio di modelli di IA per finalità generali con licenza libera e open source non rivela necessariamente informazioni sostanziali sul set di dati utilizzato per l'addestramento o il perfezionamento del modello e sulla modalità con cui è stata in tal modo garantita la conformità al diritto d'autore, l'eccezione prevista per i modelli di IA per finalità generali concernente il rispetto dei requisiti relativi alla trasparenza non dovrebbe riguardare l'obbligo di produrre una sintesi del contenuto utilizzato per l'addestramento dei modelli e l'obbligo di attuare una politica volta ad adempiere la normativa europea in materia di diritto d'autore, in particolare di individuare e rispettare la riserva dei diritti a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio¹⁵⁶.

¹⁵⁶ Direttiva (UE) 2019/790 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE (GU L 130 del 17.5.2019, pag. 92).

- (105) I modelli di IA per finalità generali, in particolare i grandi modelli di IA generativa, in grado di generare testo, immagini e altri contenuti, presentano opportunità di innovazione uniche, ma anche sfide per artisti, autori e altri creatori e per le modalità con cui i loro contenuti creativi sono creati, distribuiti, utilizzati e fruiti. Lo sviluppo e l'addestramento di tali modelli richiedono l'accesso a grandi quantità di testo, immagini, video e altri dati. Le tecniche di estrazione di testo e di dati possono essere ampiamente utilizzate in tale contesto per il reperimento e l'analisi di tali contenuti, che possono essere protetti da diritto d'autore e da diritti connessi. Qualsiasi utilizzo di contenuti protetti da diritto d'autore richiede l'autorizzazione del titolare dei diritti interessato, salvo se si applicano eccezioni e limitazioni pertinenti al diritto d'autore. La direttiva (UE) 2019/790 ha introdotto eccezioni e limitazioni che consentono, a determinate condizioni, riproduzioni ed estrazioni effettuate da opere o altri materiali ai fini dell'estrazione di testo e di dati. In base a tali norme, i titolari dei diritti hanno la facoltà di scegliere che l'utilizzo delle loro opere e di altri materiali sia da essi riservato per evitare l'estrazione di testo e di dati, salvo a fini di ricerca scientifica. Qualora il diritto di sottrarsi sia stato espressamente riservato in modo appropriato, i fornitori di modelli di IA per finalità generali devono ottenere un'autorizzazione dai titolari dei diritti, qualora intendano compiere l'estrazione di testo e di dati su tali opere.

- (106) I fornitori che immettono modelli di IA per finalità generali sul mercato dell'Unione dovrebbero garantire la conformità ai pertinenti obblighi del presente regolamento. A tal fine, i fornitori di modelli di IA per finalità generali dovrebbero mettere in atto una politica volta a rispettare il diritto dell'Unione in materia di diritto d'autore e diritti connessi, in particolare per individuare e rispettare la riserva dei diritti espresse dai titolari dei diritti a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790. Qualsiasi fornitore che immetta sul mercato dell'Unione un modello di IA per finalità generali dovrebbe rispettare tale obbligo, indipendentemente dalla giurisdizione in cui hanno luogo gli atti pertinenti in materia di diritto d'autore alla base dell'addestramento di tali modelli di IA per finalità generali. Ciò è necessario per garantire condizioni di parità tra i fornitori di modelli di IA per finalità generali, dato che nessun fornitore dovrebbe essere in grado di ottenere un vantaggio competitivo nel mercato dell'Unione applicando norme in materia di diritto d'autore meno rigorose di quelle previste nell'Unione.

- (107) Al fine di aumentare la trasparenza sui dati utilizzati nelle fasi di pre-addestramento e addestramento dei modelli di IA per finalità generali, compresi testo e dati protetti dalla normativa sul diritto d'autore, è opportuno che i fornitori di tali modelli elaborino e mettano a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali. Pur tenendo debitamente conto della necessità di proteggere i segreti commerciali e le informazioni commerciali riservate, la presente sintesi dovrebbe essere di respiro ampio e generale, anziché dettagliata sotto il profilo tecnico, al fine di agevolare le parti con interessi legittimi, compresi i titolari dei diritti d'autore, nell'esercitare e far rispettare i loro diritti ai sensi del diritto dell'Unione, ad esempio elencando le principali raccolte o serie di dati che sono state inserite nell'addestramento del modello, quali grandi banche dati o archivi di dati privati o pubblici, e fornendo una descrizione delle altre fonti di dati utilizzate. È opportuno che l'ufficio per l'IA fornisca un modello per la sintesi, che dovrebbe essere semplice ed efficace nonché consentire al fornitore di fornire la sintesi richiesta in forma descrittiva.
- (108) In merito agli obblighi imposti ai fornitori di modelli di IA per finalità generali per quanto riguarda l'attuazione di una politica volta a rispettare la normativa dell'Unione in materia di diritto d'autore e a mettere pubblicamente a disposizione una sintesi dei contenuti utilizzati per l'addestramento, l'ufficio per l'IA dovrebbe controllare se il fornitore ha adempiuto tali obblighi senza verificare o procedere a una valutazione puntuale dei dati di addestramento in termini di conformità al diritto d'autore. Il presente regolamento non pregiudica l'applicazione delle norme sul diritto d'autore previste dal diritto dell'Unione.

- (109) Il rispetto degli obblighi applicabili ai fornitori di modelli di IA per finalità generali dovrebbe essere commisurato e proporzionato al tipo di fornitore del modello, escludendo la necessità di adempimento per le persone che sviluppano o utilizzano modelli per finalità non professionali o di ricerca scientifica, le quali dovrebbero tuttavia essere incoraggiate a rispettare volontariamente tali obblighi. Fatta salva la normativa dell'Unione in materia di diritto d'autore, il rispetto di tali obblighi dovrebbe tenere debitamente conto delle dimensioni del fornitore e consentire modalità semplificate di adempimento per le PMI, comprese le start-up, che non dovrebbero comportare costi eccessivi né scoraggiare l'uso di tali modelli. In caso di modifica o perfezionamento di un modello, gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero essere limitati a tale modifica o perfezionamento, ad esempio integrando la documentazione tecnica già esistente con informazioni sulle modifiche, comprese nuove fonti di dati di addestramento, quale mezzo per adempiere gli obblighi della catena del valore di cui al presente regolamento.

(110) I modelli di IA per finalità generali potrebbero comportare rischi sistemici che includono, tra l'altro, qualsiasi effetto negativo effettivo o ragionevolmente prevedibile in relazione a incidenti gravi, perturbazioni di settori critici e serie conseguenze per la salute e la sicurezza pubbliche; eventuali effetti negativi, effettivi o ragionevolmente prevedibili, sui processi democratici e sulla sicurezza pubblica ed economica; la diffusione di contenuti illegali, mendaci o discriminatori. I rischi sistemici sono da intendersi in aumento con le capacità e la portata del modello, possono emergere durante l'intero ciclo di vita del modello e sono influenzati da condizioni di uso improprio, affidabilità, equità e sicurezza del modello, il livello di autonomia del modello, dal suo accesso agli strumenti, dalle sue modalità nuove o combinate, dalle strategie di rilascio e distribuzione, dal potenziale di rimozione delle misure protettive e da altri fattori. In particolare, gli approcci internazionali hanno finora rilevato la necessità di prestare attenzione ai rischi derivanti da potenziali usi impropri intenzionali o da involontari problemi di controllo relativi all'allineamento con l'intento umano; ai rischi chimici, biologici, radiologici e nucleari, come le modalità con cui ridurre gli ostacoli all'accesso, anche per quanto riguarda lo sviluppo e l'uso di armi o la relativa acquisizione di progetti; alle capacità informatiche offensive, come le modalità per consentire la scoperta, lo sfruttamento o l'uso operativo delle vulnerabilità; agli effetti dell'interazione e dell'uso di strumenti, compresa, ad esempio, la capacità di controllare i sistemi fisici e di interferire con infrastrutture critiche; ai rischi derivanti da modelli che realizzano copie di sé stessi o "autoreplicanti" o che addestrano altri modelli; alle modalità con cui i modelli possono dar luogo a dannosi pregiudizi e discriminazioni con rischi per gli individui, le comunità o le società; all'agevolazione della disinformazione o alla violazione della vita privata con minacce ai valori democratici e ai diritti umani; al rischio che un particolare evento possa provocare una reazione a catena con notevoli effetti negativi che potrebbero interessare fino a un'intera città, un intero settore o un'intera comunità.

- (111) È opportuno stabilire una metodologia per la classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischi sistemici. Poiché i rischi sistemici derivano da capacità particolarmente elevate, si dovrebbe considerare che un modello di IA per finalità generali presenti rischi sistemici se ha capacità di impatto elevato, valutate sulla base di metodologie e strumenti tecnici adeguati, o se ha un impatto significativo sul mercato interno a causa della sua portata. Per capacità di impatto elevato nei modelli di IA per finalità generali si intendono capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati. L'intera gamma di capacità di un modello potrebbe essere meglio compresa dopo la sua immissione sul mercato o quando i deployer interagiscono con il modello. In base allo stato dell'arte al momento dell'entrata in vigore del presente regolamento, l'importo cumulativo del calcolo utilizzato per l'addestramento del modello di IA per finalità generali misurato in operazioni in virgola mobile è una delle approssimazioni pertinenti per le capacità del modello. L'importo cumulativo del calcolo utilizzato per l'addestramento comprende il calcolo utilizzato nelle attività e nei metodi tesi a migliorare le capacità del modello prima della diffusione, quali il pre-addestramento, la generazione di dati sintetici e il perfezionamento. È pertanto opportuno fissare una soglia iniziale di operazioni in virgola mobile che, se raggiunta da un modello di IA per finalità generali, porta a presumere che il modello sia un modello di IA per finalità generali con rischi sistemici. Tale soglia dovrebbe essere adeguata nel tempo per riflettere i cambiamenti tecnologici e industriali, quali miglioramenti algoritmici o una maggiore efficienza dell'hardware, e dovrebbe essere integrata da parametri di riferimento e indicatori per la capacità del modello.

A tal fine, l'ufficio per l'IA dovrebbe dialogare con la comunità scientifica, l'industria, la società civile e altri esperti. Le soglie, nonché gli strumenti e i parametri di riferimento per la valutazione delle capacità di impatto elevato, dovrebbero essere solidi indicatori della generalità, delle capacità e del connesso rischio sistemico dei modelli di IA per finalità generali e potrebbero tenere conto delle modalità con cui il modello sarà immesso sul mercato o del numero di utenti che potrebbero esserne interessati. A integrazione di tale sistema, la Commissione dovrebbe avere la possibilità di adottare decisioni individuali per designare un modello di IA per finalità generali come modello di IA per finalità generali con rischio sistemico, qualora si accerti che tale modello abbia capacità o un impatto equivalenti a quelli rilevati dalla soglia fissata. Tale decisione dovrebbe essere adottata in base a una valutazione globale dei criteri per la designazione di un modello di IA per finalità generali con rischio sistemico di cui all'allegato del presente regolamento, come la qualità o le dimensioni del set di dati di addestramento, il numero di utenti commerciali e finali, le sue modalità di input e output, il suo livello di autonomia e scalabilità o gli strumenti a cui ha accesso. Su richiesta motivata di un fornitore il cui modello è stato designato come modello di IA per finalità generali con rischio sistemico, la Commissione dovrebbe tenere conto della richiesta e può decidere di rivalutare se si possa ancora ritenere che il modello di IA per finalità generali presenti rischi sistemici.

(112) È altresì opportuno specificare una procedura per la classificazione di un modello di IA per finalità generali con rischi sistemici. Si dovrebbe presumere che un modello di IA per finalità generali che raggiunge la soglia applicabile per le capacità di impatto elevato sia un modello di IA per finalità generali con rischio sistemico. Il fornitore dovrebbe informare l'ufficio per l'IA al più tardi due settimane dopo che i requisiti sono soddisfatti o quando viene a conoscenza del fatto che un modello di IA per finalità generali soddisferà i requisiti che portano alla suddetta presunzione. Questo assume particolare rilevanza in relazione alla soglia di operazioni in virgola mobile, dato che l'addestramento dei modelli di IA per finalità generali richiede una pianificazione considerevole, comprensiva dell'assegnazione anticipata delle risorse di calcolo, cosicché i fornitori di modelli di IA per finalità generali siano in grado di sapere se il loro modello può raggiungere la soglia prima della conclusione dell'addestramento. Nel contesto di tale notifica, il fornitore dovrebbe essere in grado di dimostrare che, a causa delle sue caratteristiche specifiche, un modello di IA per finalità generali non presenta eccezionalmente rischi sistemici e che, pertanto, non dovrebbe essere classificato come modello di IA per finalità generali con rischi sistemici. Si tratta di informazioni utili all'ufficio per l'IA per anticipare l'immissione sul mercato di modelli di IA per finalità generali con rischi sistemici e i fornitori possono iniziare a dialogare con l'ufficio per l'IA sin dalle prime fasi. Tali informazioni sono particolarmente importanti per quanto riguarda i modelli di IA per finalità generali che si pianifica di rilasciare come open source, dato che, dopo il rilascio del modello open source, è possibile che sia più difficile attuare le misure necessarie a garantire il rispetto degli obblighi di cui al presente regolamento.

- (113) La Commissione dovrebbe avere il potere di designare un modello di IA per finalità generali come modello di IA per finalità generali con rischio sistemico, se viene a conoscenza del fatto che il modello in questione soddisfa i requisiti per tale designazione e in precedenza tale fatto non era noto o il pertinente fornitore aveva omesso di notificarlo alla Commissione. Un sistema di segnalazioni qualificate dovrebbe garantire che l'ufficio per l'IA sia informato dal gruppo scientifico dei modelli di IA per finalità generali che potrebbero dover essere classificati come modelli di IA per finalità generali con rischio sistemico, in aggiunta alle attività di monitoraggio dell'ufficio per l'IA.
- (114) I fornitori di modelli di IA per finalità generali che presentano rischi sistemici dovrebbero essere soggetti, oltre agli obblighi previsti per i fornitori di modelli di IA per finalità generali, agli obblighi volti a individuare e attenuare tali rischi e a garantire un livello adeguato di protezione della cibersicurezza, a prescindere dal fatto che il modello sia fornito come modello autonomo o integrato in un sistema di IA o in un prodotto. Per conseguire tali obiettivi, il presente regolamento dovrebbe imporre ai fornitori di effettuare le necessarie valutazioni dei modelli, in particolare prima della sua prima immissione sul mercato, compreso lo svolgimento e la documentazione del test contraddittorio (adversarial testing) dei modelli, anche, se del caso, mediante prove interne o esterne indipendenti. Inoltre, i fornitori di modelli di IA per finalità generali con rischi sistemici dovrebbero valutare e attenuare continuamente i rischi sistemici, ad esempio attuando politiche di gestione dei rischi, quali processi di responsabilità e governance, svolgendo il monitoraggio successivo all'immissione sul mercato, adottando misure adeguate lungo l'intero ciclo di vita del modello e cooperando con gli attori pertinenti lungo la catena del valore dell'IA.

- (115) I fornitori di modelli di IA per finalità generali con rischi sistemici dovrebbero valutare e attenuare i possibili rischi sistemici. Se lo sviluppo o l'utilizzo di un modello di IA per finalità generali che potrebbe presentare rischi sistemici causa un incidente grave, nonostante gli sforzi volti a individuare e prevenire i rischi connessi a tale modello, il fornitore del modello di IA per finalità generali dovrebbe, senza indebito ritardo, tenere traccia dell'incidente e riferire alla Commissione e alle autorità nazionali competenti le informazioni pertinenti e le eventuali misure correttive. Inoltre, i fornitori dovrebbero garantire un livello adeguato di protezione della cibersecurity per il modello e la sua infrastruttura fisica, se del caso, lungo l'intero ciclo di vita del modello. La protezione della cibersecurity connessa ai rischi sistemici associati a uso doloso o attacchi dovrebbe tenere debitamente in considerazione model leakage accidentali, rilasci non autorizzati, elusioni delle misure di sicurezza, nonché la difesa contro gli attacchi informatici, l'accesso non autorizzato o il furto di modelli. Tale protezione potrebbe essere facilitata mettendo al sicuro pesi, algoritmi, server e set di dati relativi al modello, ad esempio attraverso misure di sicurezza operativa per la sicurezza delle informazioni, politiche specifiche in materia di cibersecurity, soluzioni tecniche e consolidate appropriate e controlli dell'accesso informatico e fisico, che siano adeguati alle circostanze pertinenti e ai rischi connessi.

- (116) L'ufficio per l'IA dovrebbe incoraggiare e agevolare l'elaborazione, il riesame e l'adeguamento dei codici di buone pratiche, tenendo conto degli approcci internazionali. Tutti i fornitori di modelli di IA per finalità generali potrebbero essere invitati a partecipare. Per garantire che i codici di buone pratiche riflettano lo stato dell'arte e tengano debitamente conto di una serie diversificata di prospettive, l'ufficio per l'IA dovrebbe collaborare con le pertinenti autorità nazionali competenti e potrebbe, se del caso, consultare le organizzazioni della società civile e altri portatori di interessi ed esperti pertinenti, compreso il gruppo di esperti scientifici, ai fini dell'elaborazione di tali codici. I codici di buone pratiche dovrebbero disciplinare gli obblighi per i fornitori di modelli di IA per finalità generali e per i fornitori di modelli di IA per finalità generali che presentano rischi sistemici. Inoltre, quanto ai rischi sistemici, i codici di buone pratiche dovrebbero contribuire a stabilire una tassonomia del tipo e della natura dei rischi sistemici a livello dell'Unione, comprese le loro fonti. I codici di buone pratiche dovrebbero inoltre concentrarsi su misure specifiche di valutazione e attenuazione dei rischi.

- (117) I codici di buone pratiche dovrebbero rappresentare uno strumento essenziale per i fornitori di modelli di IA per finalità generali ai fini di un'adeguata conformità agli obblighi previsti dal presente regolamento. I fornitori dovrebbero poter fare affidamento su codici di buone pratiche per dimostrare la conformità agli obblighi. Mediante atti di esecuzione, la Commissione può decidere di approvare un codice di buone pratiche e conferire ad esso una validità generale all'interno dell'Unione o, in alternativa, di stabilire norme comuni per l'attuazione dei pertinenti obblighi, qualora un codice di buone pratiche non possa essere portato a termine o ritenuto adeguato da parte dell'ufficio per l'IA entro la data di applicazione del presente regolamento. Quando una norma armonizzata è pubblicata e ritenuta idonea a disciplinare i pertinenti obblighi da parte dell'ufficio per l'IA, la conformità a una norma armonizzata europea dovrebbe conferire ai fornitori la presunzione di conformità. I fornitori di modelli di IA per finalità generali dovrebbero inoltre essere in grado di dimostrare la conformità utilizzando mezzi adeguati alternativi, se non sono disponibili codici di buone pratiche o norme armonizzate, oppure se tali fornitori scelgono di non fare affidamento su tali codici e norme.

(118) Il presente regolamento disciplina i sistemi di IA e i modelli di IA imponendo determinati requisiti e obblighi agli operatori del mercato pertinenti che li immettono sul mercato, li mettono in servizio o li utilizzano nell'Unione, integrando in tal modo gli obblighi per i prestatori di servizi intermediari che incorporano tali sistemi o modelli nei loro servizi disciplinati dal regolamento (UE) 2022/2065. Nella misura in cui sono integrati in piattaforme online di dimensioni molto grandi designate o motori di ricerca online di dimensioni molto grandi designati, tali sistemi o modelli sono soggetti al quadro di gestione dei rischi di cui al regolamento (UE) 2022/2065. Di conseguenza, si dovrebbe ritenere che gli obblighi corrispondenti del presente regolamento siano adempiuti, salvo se emergono e sono individuati in tali modelli dei rischi sistemici significativi non disciplinati dal regolamento (UE) 2022/2065. In tale quadro, i prestatori di piattaforme online di dimensioni molto grandi e motori di ricerca online di dimensioni molto grandi sono tenuti a valutare i potenziali rischi sistemici derivanti dalla progettazione, dal funzionamento e dall'utilizzo dei rispettivi servizi, comprese le modalità con cui la progettazione dei sistemi algoritmici impiegati nel servizio possono contribuire a tali rischi, nonché i rischi sistemici derivanti da potenziali usi impropri. Tali prestatori sono altresì tenuti ad adottare misure di attenuazione adeguate nel rispetto dei diritti fondamentali.

- (119) Considerando la rapidità dell'innovazione e dell'evoluzione tecnologica dei servizi digitali che rientrano nell'ambito di applicazione dei diversi strumenti previsti dal diritto dell'Unione, in particolare tenendo presente l'uso e la percezione dei loro destinatari, i sistemi di IA soggetti al presente regolamento possono essere forniti come servizi intermediari o parti di essi ai sensi del regolamento (UE) 2022/2065, da interpretarsi in modo tecnologicamente neutro. Ad esempio, i sistemi di IA possono essere utilizzati per fornire motori di ricerca online, in particolare nella misura in cui un sistema di IA, come un chatbot online, effettua ricerche, in linea di principio, su tutti i siti web, incorpora i risultati nelle sue conoscenze esistenti e si avvale delle conoscenze aggiornate per generare un unico output che combina diverse fonti di informazione.
- (120) Inoltre, gli obblighi imposti dal presente regolamento ai fornitori e ai deployer di taluni sistemi di IA, volti a consentire il rilevamento e la divulgazione del fatto che gli output di tali sistemi siano generati o manipolati artificialmente, sono molto importanti per contribuire all'efficace attuazione del regolamento (UE) 2022/2065. Ciò si applica specialmente agli obblighi per i fornitori di piattaforme online di dimensioni molto grandi o motori di ricerca online di dimensioni molto grandi di individuare e attenuare i rischi sistemici che possono derivare dalla diffusione di contenuti generati o manipolati artificialmente, in particolare il rischio di impatti negativi effettivi o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, anche mediante la disinformazione.

(121) La normazione dovrebbe svolgere un ruolo fondamentale nel fornire soluzioni tecniche ai fornitori per garantire la conformità al presente regolamento, in linea con lo stato dell'arte, e promuovere l'innovazione, la competitività e la crescita nel mercato unico. La conformità alle norme armonizzate quali definite all'articolo 2, punto 1, lettera c), del regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio¹⁵⁷, le quali normalmente dovrebbero rispecchiare lo stato dell'arte, dovrebbe essere un modo per i fornitori di dimostrare la conformità ai requisiti del presente regolamento. È pertanto opportuno incoraggiare una rappresentanza equilibrata degli interessi che coinvolga tutti i portatori di interessi pertinenti nell'elaborazione delle norme, in particolare le PMI, le organizzazioni dei consumatori e i portatori di interessi in materia sociale e ambientale conformemente agli articoli 5 e 6 del regolamento (UE) n. 1025/2012. Al fine di agevolare l'adempimento, le richieste di normazione dovrebbero essere presentate dalla Commissione senza indebito ritardo. In sede di elaborazione della richiesta di normazione, la Commissione dovrebbe consultare il forum consultivo e il consiglio per l'IA al fine di ottenere le competenze pertinenti. Tuttavia, in assenza di riferimenti pertinenti a norme armonizzate, la Commissione dovrebbe poter stabilire, mediante atti di esecuzione e previa consultazione del forum consultivo, specifiche comuni per determinati requisiti previsti del presente regolamento.

¹⁵⁷ Regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, sulla normazione europea, che modifica le direttive 89/686/CEE e 93/15/CEE del Consiglio nonché le direttive 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE del Parlamento europeo e del Consiglio e che abroga la decisione 87/95/CEE del Consiglio e la decisione n. 1673/2006/CE del Parlamento europeo e del Consiglio (GU L 316 del 14.11.2012, pag. 12).

La specifica comune dovrebbe costituire una soluzione eccezionale di ripiego per agevolare l'obbligo del fornitore di conformarsi ai requisiti del presente regolamento, quando la richiesta di normazione non è stata accettata da alcuna delle organizzazioni europee di normazione, quando le pertinenti norme armonizzate non tengono sufficientemente conto delle preoccupazioni in materia di diritti fondamentali, quando le norme armonizzate non sono conformi alla richiesta o quando vi sono ritardi nell'adozione di una norma armonizzata appropriata. Qualora tale ritardo nell'adozione di una norma armonizzata sia dovuto alla complessità tecnica di tale norma, la Commissione dovrebbe tenerne conto prima di prendere in considerazione la definizione di specifiche comuni. Nell'elaborare specifiche comuni, la Commissione è incoraggiata a cooperare con i partner internazionali e gli organismi internazionali di normazione.

- (122) È opportuno che, fatto salvo il ricorso a norme armonizzate e specifiche comuni, i fornitori di un sistema di IA ad alto rischio che è stato addestrato e sottoposto a prova con dati che rispecchiano il contesto geografico, comportamentale, contestuale o funzionale specifico all'interno del quale il sistema di IA è destinato a essere usato si presumano conformi alla misura pertinente prevista dal requisito in materia di governance dei dati di cui al presente regolamento. Fatti salvi i requisiti relativi alla robustezza e all'accuratezza di cui al presente regolamento, conformemente all'articolo 54, paragrafo 3, del regolamento (UE) 2019/881, i sistemi di IA ad alto rischio certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersecurity a norma di tale regolamento e i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* dovrebbero essere considerati conformi al requisito di cibersecurity di cui al presente regolamento nella misura in cui il certificato di cibersecurity o la dichiarazione di conformità o parti di essi contemplino il requisito di cibersecurity di cui al presente regolamento. Ciò lascia impregiudicata la natura volontaria di tale sistema di cibersecurity.
- (123) Al fine di garantire un elevato livello di affidabilità dei sistemi di IA ad alto rischio, è opportuno sottoporre tali sistemi a una valutazione della conformità prima della loro immissione sul mercato o messa in servizio.

- (124) Al fine di ridurre al minimo l'onere per gli operatori ed evitare eventuali duplicazioni, la conformità ai requisiti del presente regolamento dei sistemi di IA ad alto rischio collegati a prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione basata sul nuovo quadro legislativo dovrebbe essere valutata nell'ambito della valutazione della conformità già prevista da tale normativa. L'applicabilità dei requisiti del presente regolamento non dovrebbe pertanto incidere sulla logica, la metodologia o la struttura generale specifiche della valutazione della conformità a norma della pertinente normativa di armonizzazione dell'Unione.
- (125) Data la complessità dei sistemi di IA ad alto rischio e i rischi ad essi associati, è importante sviluppare un'adeguata procedura di valutazione della conformità per quanto riguarda i sistemi di IA ad alto rischio che coinvolgono organismi notificati, la cosiddetta valutazione della conformità da parte di terzi. Tuttavia, in considerazione dell'attuale esperienza dei certificatori professionali pre-commercializzazione nel settore della sicurezza dei prodotti e della diversa natura dei rischi connessi, è opportuno limitare, almeno in una fase iniziale di applicazione del presente regolamento, l'ambito di applicazione della valutazione della conformità da parte di terzi ai sistemi di IA ad alto rischio diversi da quelli collegati ai prodotti. È pertanto opportuno che la valutazione della conformità di tali sistemi sia generalmente effettuata dal fornitore sotto la propria responsabilità, con la sola eccezione dei sistemi di IA destinati a essere utilizzati per la biometrica.

- (126) Ai fini delle valutazioni della conformità da parte di terzi, laddove richieste, è opportuno che le autorità nazionali competenti notifichino gli organismi notificati a norma del presente regolamento, a condizione che tali organismi soddisfino una serie di requisiti, in particolare in materia di indipendenza, competenza, assenza di conflitti di interesse e requisiti idonei di cibersecurity. La notifica di tali organismi dovrebbe essere trasmessa dalle autorità nazionali competenti alla Commissione e agli altri Stati membri mediante lo strumento elettronico di notifica elaborato e gestito dalla Commissione a norma dell'allegato I, articolo R23, della decisione n. 768/2008/CE.
- (127) In linea con gli impegni assunti dall'Unione nell'ambito dell'accordo dell'Organizzazione mondiale del commercio sugli ostacoli tecnici agli scambi, è opportuno agevolare il riconoscimento reciproco dei risultati della valutazione della conformità prodotti da organismi di valutazione della conformità competenti, indipendentemente dal luogo in cui siano stabiliti, purché tali organismi di valutazione della conformità istituiti a norma del diritto di un paese terzo soddisfino i requisiti applicabili del presente regolamento e l'Unione abbia concluso un accordo in tal senso. In questo contesto, la Commissione dovrebbe esplorare attivamente possibili strumenti internazionali a tale scopo e, in particolare, perseguire la conclusione di accordi di riconoscimento reciproco con i paesi terzi.

- (128) In linea con la nozione generalmente riconosciuta di modifica sostanziale dei prodotti disciplinati dalla normativa di armonizzazione dell'Unione, è opportuno che ogniqualvolta intervenga una modifica che possa incidere sulla conformità del sistema di IA ad alto rischio al presente regolamento (ad esempio, la modifica del sistema operativo o dell'architettura del software), oppure quando viene modificata la finalità prevista del sistema, tale sistema di IA sia considerato un nuovo sistema di IA che dovrebbe essere sottoposto a una nuova valutazione della conformità. Tuttavia, le modifiche apportate all'algoritmo e alle prestazioni dei sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio, in particolare adattando automaticamente le modalità di svolgimento delle funzioni, non dovrebbero costituire una modifica sostanziale, a condizione che tali modifiche siano state predeterminate dal fornitore e valutate al momento della valutazione della conformità.
- (129) I sistemi di IA ad alto rischio dovrebbero recare la marcatura CE per indicare la loro conformità al presente regolamento, in modo da poter circolare liberamente nel mercato interno. Per i sistemi di IA ad alto rischio integrati in un prodotto, dovrebbe essere apposta una marcatura CE fisica, integrabile con una marcatura CE digitale. Per i sistemi di IA ad alto rischio forniti solo digitalmente, dovrebbe essere utilizzata una marcatura CE digitale. Gli Stati membri non dovrebbero ostacolare in maniera ingiustificata l'immissione sul mercato o la messa in servizio di sistemi di IA ad alto rischio che soddisfano i requisiti stabiliti nel presente regolamento e recano la marcatura CE.

- (130) La disponibilità in tempi rapidi di tecnologie innovative può, a determinate condizioni, essere fondamentale per la salute e la sicurezza delle persone, per la tutela dell'ambiente e la protezione dai cambiamenti climatici e per la società nel suo insieme. È pertanto opportuno che, per motivi eccezionali di pubblica sicurezza o di tutela della vita e della salute delle persone fisiche, di tutela dell'ambiente nonché di protezione dei principali beni industriali e infrastrutturali, le autorità di vigilanza del mercato possano autorizzare l'immissione sul mercato o la messa in servizio di sistemi di IA che non sono stati sottoposti a una valutazione della conformità. In situazioni debitamente giustificate come previsto dal presente regolamento, le autorità di contrasto o le autorità di protezione civile possono mettere in servizio uno specifico sistema di IA ad alto rischio senza l'autorizzazione dell'autorità di vigilanza del mercato, a condizione che tale autorizzazione sia richiesta durante o dopo l'uso senza indebito ritardo.
- (131) Al fine di agevolare il lavoro della Commissione e degli Stati membri nel settore dell'IA e di aumentare la trasparenza nei confronti del pubblico, è opportuno che i fornitori di sistemi di IA ad alto rischio diversi da quelli collegati a prodotti che rientrano nell'ambito di applicazione della pertinente normativa di armonizzazione dell'Unione vigente, nonché i fornitori che ritengono che, in base a una deroga, il sistema di IA elencato tra i casi ad alto rischio nell'allegato del presente regolamento non sia ad alto rischio, siano tenuti a registrarsi e a registrare informazioni sul loro sistema di IA in una banca dati dell'UE, che sarà istituita e gestita dalla Commissione. Prima di utilizzare un sistema di IA elencato tra i casi ad alto rischio nell'allegato del presente regolamento, i deployer di sistemi di IA ad alto rischio che sono autorità, agenzie o organismi pubblici dovrebbero registrarsi in tale banca dati e selezionare il sistema che intendono utilizzare.

Gli altri deployer dovrebbero essere autorizzati a farlo su base volontaria. Questa sezione della banca dati dell'UE dovrebbe essere accessibile al pubblico gratuitamente e le informazioni dovrebbero essere di facile consultazione, comprensibili e leggibili meccanicamente. La banca dati dell'UE dovrebbe inoltre essere di facile utilizzo, ad esempio tramite la fornitura di funzionalità di ricerca, anche attraverso parole chiave, che consentano al pubblico di reperire informazioni pertinenti da presentare al momento della registrazione dei sistemi di IA ad alto rischio e riguardanti l'uso di sistemi di IA ad alto rischio, elencati in allegato al presente regolamento, a cui corrispondono i sistemi di IA ad alto rischio. Qualsiasi modifica sostanziale dei sistemi di IA ad alto rischio dovrebbe essere registrata anche nella banca dati dell'UE. Per i sistemi di IA ad alto rischio nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, gli obblighi di registrazione dovrebbero essere adempiuti in una sezione non pubblica sicura della banca dati dell'UE. L'accesso alla sezione non pubblica sicura dovrebbe essere strettamente limitato alla Commissione e alle autorità di vigilanza del mercato per quanto riguarda la rispettiva sezione nazionale di tale banca dati. I sistemi di IA ad alto rischio nel settore delle infrastrutture critiche dovrebbero essere registrati solo a livello nazionale. È opportuno che la Commissione sia la titolare del trattamento di tale banca dati dell'UE conformemente al regolamento (UE) 2018/1725. Al fine di garantire la piena funzionalità della banca dati dell'UE, è opportuno che, al momento dell'attivazione, la procedura per l'istituzione della banca dati preveda l'elaborazione di specifiche funzionali da parte della Commissione e una relazione di audit indipendente. Nello svolgimento dei suoi compiti di titolare del trattamento dei dati nella banca dati dell'UE, la Commissione dovrebbe tenere conto dei rischi legati alla cbersicurezza. Onde massimizzare la disponibilità e l'uso della banca dati dell'UE da parte del pubblico, la banca dati dell'UE, comprese le informazioni ivi messe a disposizione, dovrebbe essere conforme ai requisiti di cui alla direttiva (UE) 2019/882.

- (132) Alcuni sistemi di IA destinati all'interazione con persone fisiche o alla generazione di contenuti possono comportare rischi specifici di impersonificazione o inganno, a prescindere dal fatto che siano considerati ad alto rischio o no. L'uso di tali sistemi dovrebbe pertanto essere, in determinate circostanze, soggetto a specifici obblighi di trasparenza, fatti salvi i requisiti e gli obblighi per i sistemi di IA ad alto rischio, e soggetto ad eccezioni mirate per tenere conto delle particolari esigenze delle attività di contrasto. Le persone fisiche dovrebbero in particolare ricevere una notifica nel momento in cui interagiscono con un sistema di IA, a meno che tale interazione non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. Nell'attuare tale obbligo, le caratteristiche delle persone fisiche appartenenti a gruppi vulnerabili a causa della loro età o disabilità dovrebbero essere prese in considerazione nella misura in cui il sistema di IA sia destinato a interagire anche con tali gruppi. È inoltre opportuno che le persone fisiche ricevano una notifica quando sono esposte a sistemi di IA che, nel trattamento dei loro dati biometrici, possono identificare o inferire le emozioni o intenzioni di tali persone o assegnarle a categorie specifiche. Tali categorie specifiche possono riguardare aspetti quali il sesso, l'età, il colore dei capelli, il colore degli occhi, i tatuaggi, i tratti personali, l'origine etnica, le preferenze e gli interessi personali. Tali informazioni e notifiche dovrebbero essere fornite in formati accessibili alle persone con disabilità.

(133) Diversi sistemi di IA possono generare grandi quantità di contenuti sintetici, che per gli esseri umani è divenuto sempre più difficile distinguere dai contenuti autentici e generati da esseri umani. L'ampia disponibilità e l'aumento delle capacità di tali sistemi hanno un impatto significativo sull'integrità e sulla fiducia nell'ecosistema dell'informazione, aumentando i nuovi rischi di cattiva informazione e manipolazione su vasta scala, frode, impersonificazione e inganno dei consumatori. Alla luce di tali impatti, della rapida evoluzione tecnologica e della necessità di nuovi metodi e tecniche per risalire all'origine delle informazioni, è opportuno imporre ai fornitori di tali sistemi di integrare soluzioni tecniche che consentano agli output di essere marcati in un formato leggibile meccanicamente e di essere rilevabili come generati o manipolati da un sistema di IA e non da esseri umani. Tali tecniche e metodi dovrebbero essere sufficientemente affidabili, interoperabili, efficaci e solidi nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle tecniche disponibili o di una combinazione di tali tecniche, quali filigrane, identificazioni di metadati, metodi crittografici per dimostrare la provenienza e l'autenticità dei contenuti, metodi di registrazione, impronte digitali o altre tecniche, a seconda dei casi. Nell'attuare tale obbligo, i fornitori dovrebbero tenere conto anche delle specificità e dei limiti dei diversi tipi di contenuti e dei pertinenti sviluppi tecnologici e di mercato nel settore, come rispecchia lo stato dell'arte generalmente riconosciuto. Tali tecniche e metodi possono essere attuati a livello di sistema di IA o a livello di modello di IA, compresi i modelli di IA per finalità generali che generano contenuti, facilitando in tal modo l'adempimento di tale obbligo da parte del fornitore a valle del sistema di IA. Per continuare a essere proporzionato, è opportuno prevedere che tale obbligo di marcatura non debba riguardare i sistemi di IA che svolgono principalmente una funzione di assistenza per l'editing standard o i sistemi di IA che non modificano in modo sostanziale i dati di input forniti dal deployer o la rispettiva semantica.

- (134) Oltre alle soluzioni tecniche utilizzate dai fornitori del sistema di IA, i deployer che utilizzano un sistema di IA per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi, entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri a una persona (deep fake), dovrebbero anche rendere noto in modo chiaro e distinto che il contenuto è stato creato o manipolato artificialmente etichettando di conseguenza gli output dell'IA e rivelandone l'origine artificiale. L'adempimento di tale obbligo di trasparenza non dovrebbe essere interpretato nel senso che l'uso del sistema di IA o dei suoi output ostacola il diritto alla libertà di espressione e il diritto alla libertà delle arti e delle scienze garantito dalla Carta, in particolare quando il contenuto fa parte di un'opera o di un programma manifestamente creativo, satirico, artistico, fittizio, o analogo fatte salve le tutele adeguate per i diritti e le libertà dei terzi. In tali casi, l'obbligo di trasparenza per i deep fake di cui al presente regolamento si limita alla rivelazione dell'esistenza di tali contenuti generati o manipolati in modo adeguato che non ostacoli l'esposizione o il godimento dell'opera, compresi il suo normale sfruttamento e utilizzo, mantenendo nel contempo l'utilità e la qualità dell'opera. È inoltre opportuno prevedere un obbligo di divulgazione analogo in relazione al testo generato o manipolato dall'IA nella misura in cui è pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico, a meno che il contenuto generato dall'IA sia stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica abbia la responsabilità editoriale della pubblicazione del contenuto.

- (135) Fatta salva la natura obbligatoria e la piena applicabilità degli obblighi di trasparenza, la Commissione può altresì incoraggiare e agevolare l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi in materia di rilevazione ed etichettatura dei contenuti generati o manipolati artificialmente, anche per sostenere modalità pratiche per rendere accessibili, se del caso, i meccanismi di rilevazione e favorire la cooperazione con altri attori lungo la catena del valore, diffondere contenuti o verificarne l'autenticità e la provenienza onde consentire al pubblico di distinguere efficacemente i contenuti generati dall'IA.
- (136) Gli obblighi imposti dal presente regolamento ai fornitori e ai deployer di taluni sistemi di IA, volti a consentire il rilevamento e la divulgazione del fatto che gli output di tali sistemi siano generati o manipolati artificialmente, sono molto importanti per contribuire all'efficace attuazione del regolamento (UE) 2022/2065. Ciò si applica specialmente agli obblighi per i fornitori di piattaforme online di dimensioni molto grandi o motori di ricerca online di dimensioni molto grandi di individuare e attenuare i rischi sistemici che possono derivare dalla diffusione di contenuti generati o manipolati artificialmente, in particolare il rischio di impatti negativi effettivi o prevedibili sui processi democratici, sul dibattito civico e sui processi elettorali, anche mediante la disinformazione. L'obbligo di etichettare i contenuti generati dai sistemi di IA a norma del presente regolamento lascia impregiudicato l'obbligo di cui all'articolo 16, paragrafo 6, del regolamento (UE) 2022/2065 per i prestatori di servizi di memorizzazione di informazioni di trattare le segnalazioni di contenuti illegali ricevute a norma dell'articolo 16, paragrafo 1, di tale regolamento e non dovrebbe influenzare la valutazione e la decisione in merito all'illegalità del contenuto specifico. Tale valutazione dovrebbe essere effettuata solo con riferimento alle norme che disciplinano la legalità dei contenuti.

- (137) La conformità agli obblighi di trasparenza per i sistemi di IA disciplinati dal presente regolamento non dovrebbe essere interpretata nel senso che l'uso del sistema di IA o dei suoi output è lecito ai sensi del presente regolamento o di altre disposizioni del diritto dell'Unione e degli Stati membri e dovrebbe lasciare impregiudicati gli altri obblighi di trasparenza per i deployer dei sistemi di IA stabiliti dal diritto dell'Unione o nazionale.
- (138) L'IA è una famiglia di tecnologie in rapida evoluzione che richiede sorveglianza regolamentare e uno spazio sicuro e controllato per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi. Al fine di garantire un quadro giuridico che promuova l'innovazione, sia adeguato alle esigenze future e resiliente alle perturbazioni, gli Stati membri dovrebbero garantire che le rispettive autorità nazionali competenti istituiscano almeno uno spazio di sperimentazione normativa in materia di IA a livello nazionale per agevolare lo sviluppo e le prove di sistemi di IA innovativi, sotto una rigorosa sorveglianza regolamentare, prima che tali sistemi siano immessi sul mercato o altrimenti messi in servizio. Gli Stati membri potrebbero inoltre adempiere tale obbligo partecipando a spazi di sperimentazione normativa già esistenti o istituendo congiuntamente uno spazio di sperimentazione con le autorità competenti di uno o più Stati membri, nella misura in cui tale partecipazione fornisca un livello equivalente di copertura nazionale per gli Stati membri partecipanti. Gli spazi di sperimentazione normativa per l'IA potrebbero essere istituiti in forma fisica, digitale o ibrida e potrebbero accogliere prodotti sia fisici che digitali. Le autorità costituenti dovrebbero altresì garantire che gli spazi di sperimentazione normativa per l'IA dispongano delle risorse adeguate per il loro funzionamento, comprese risorse finanziarie e umane.

(139) Gli obiettivi degli spazi di sperimentazione normativa per l'IA dovrebbero essere la promozione dell'innovazione in materia di IA, mediante la creazione di un ambiente controllato di sperimentazione e prova nella fase di sviluppo e pre-commercializzazione al fine di garantire la conformità dei sistemi di IA innovativi al presente regolamento e ad altre pertinenti disposizioni di diritto dell'Unione e nazionale. Inoltre, gli spazi di sperimentazione normativa per l'IA dovrebbero avere come obiettivo il rafforzamento della certezza del diritto per gli innovatori e della sorveglianza e della comprensione da parte delle autorità competenti delle opportunità, dei rischi emergenti e degli impatti dell'uso dell'IA, l'agevolazione dell'apprendimento normativo per le autorità e le imprese, anche in vista del futuro adeguamento del quadro giuridico, il sostegno alla cooperazione e la condivisione delle migliori pratiche con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA, nonché l'accelerazione dell'accesso ai mercati, anche mediante l'eliminazione degli ostacoli per le PMI, comprese le start-up. Gli spazi di sperimentazione normativa per l'IA dovrebbero essere ampiamente disponibili in tutta l'Unione e si dovrebbe prestare particolare attenzione alla loro accessibilità per le PMI, comprese le start-up. La partecipazione allo spazio di sperimentazione normativa per l'IA dovrebbe concentrarsi su questioni che creano incertezza giuridica rendendo difficoltoso per i fornitori e i potenziali fornitori innovare, sperimentare l'IA nell'Unione e contribuire all'apprendimento normativo basato su dati concreti. La supervisione dei sistemi di IA nello spazio di sperimentazione normativa per l'IA dovrebbe pertanto riguardare il relativo sviluppo, addestramento, prova e convalida prima che i sistemi siano immessi sul mercato o messi in servizio, nonché la nozione e il verificarsi di modifiche sostanziali che possono richiedere una nuova procedura di valutazione della conformità. Qualsiasi rischio significativo individuato durante lo sviluppo e le prove di tali sistemi di IA dovrebbe comportare l'adozione di adeguate misure di attenuazione e, in mancanza di ciò, la sospensione del processo di sviluppo e di prova.

Se del caso, le autorità nazionali competenti che istituiscono spazi di sperimentazione normativa per l'IA dovrebbero cooperare con altre autorità pertinenti, comprese quelle che vigilano sulla protezione dei diritti fondamentali, e potrebbero consentire il coinvolgimento di altri attori all'interno dell'ecosistema dell'IA, quali organizzazioni di normazione nazionali o europee, organismi notificati, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione, poli europei dell'innovazione digitale e pertinenti portatori di interessi e organizzazioni della società civile. Al fine di garantire un'attuazione uniforme in tutta l'Unione e le economie di scala, è opportuno stabilire regole comuni per l'attuazione degli spazi di sperimentazione normativa per l'IA e un quadro per la cooperazione tra le autorità competenti coinvolte nel controllo degli spazi di sperimentazione. Gli spazi di sperimentazione normativa per l'IA istituiti a norma del presente regolamento non dovrebbero pregiudicare altre disposizioni che consentono la creazione di altri spazi di sperimentazione volti a garantire la conformità a disposizioni del diritto diverse dal presente regolamento. Se del caso, le pertinenti autorità competenti responsabili di tali altri spazi di sperimentazione normativa dovrebbero considerare i vantaggi derivanti dall'utilizzo di tali spazi di sperimentazione anche al fine di garantire la conformità dei sistemi di IA al presente regolamento. Previo accordo tra le autorità nazionali competenti e i partecipanti allo spazio di sperimentazione normativa per l'IA, anche le prove in condizioni reali possono essere gestite e supervisionate nel quadro dello spazio di sperimentazione normativa per l'IA.

- (140) Il presente regolamento dovrebbe fornire la base giuridica ai fornitori e ai potenziali fornitori nello spazio di sperimentazione normativa per l'IA per utilizzare i dati personali raccolti per altre finalità ai fini dello sviluppo di determinati sistemi di IA di interesse pubblico nell'ambito dello spazio di sperimentazione normativa per l'IA, solo a specifiche condizioni, conformemente all'articolo 6, paragrafo 4, e all'articolo 9, paragrafo 2, lettera g), del regolamento (UE) 2016/679, e agli articoli 5, 6 e 10 del regolamento (UE) 2018/1725, e fatti salvi l'articolo 4, paragrafo 2, e l'articolo 10 della direttiva (UE) 2016/680. Tutti gli altri obblighi dei titolari del trattamento e i diritti degli interessati ai sensi del regolamento (UE) 2016/679, del regolamento (UE) 2018/1725 e della direttiva (UE) 2016/680 restano applicabili. In particolare, il presente regolamento non dovrebbe costituire una base giuridica ai sensi dell'articolo 22, paragrafo 2, lettera b), del regolamento (UE) 2016/679 e dell'articolo 24, paragrafo 2, lettera b), del regolamento (UE) 2018/1725. I fornitori e i potenziali fornitori nello spazio di sperimentazione normativa per l'IA dovrebbero fornire garanzie adeguate e cooperare con le autorità competenti, anche seguendo i loro orientamenti e agendo rapidamente e in buona fede per attenuare adeguatamente eventuali rischi significativi individuati per la sicurezza, la salute e i diritti fondamentali che possono emergere durante lo sviluppo, le prove e la sperimentazione in tale spazio.

(141) Al fine di accelerare il processo di sviluppo e immissione sul mercato dei sistemi di IA ad alto rischio elencati in un allegato del presente regolamento, è importante che anche i fornitori o i potenziali fornitori di tali sistemi possano beneficiare di un regime specifico per sottoporre a prova tali sistemi in condizioni reali, senza partecipare a uno spazio di sperimentazione normativa per l'IA. Tuttavia, in tali casi, e tenendo conto delle possibili conseguenze di tali prove sulle persone, è opportuno garantire che il presente regolamento introduca garanzie e condizioni adeguate e sufficienti per i fornitori o potenziali fornitori. Tali garanzie dovrebbero includere, tra l'altro, la richiesta del consenso informato delle persone fisiche a partecipare a prove in condizioni reali, ad eccezione delle autorità di contrasto quando la richiesta di consenso informato impedirebbe di sottoporre a prova il sistema di IA. Il consenso dei soggetti a partecipare a tali prove a norma del presente regolamento è distinto e non pregiudica il consenso degli interessati al trattamento dei loro dati personali ai sensi della pertinente normativa in materia di protezione dei dati.

È inoltre importante ridurre al minimo i rischi e consentire la sorveglianza da parte delle autorità competenti e richiedere pertanto ai potenziali fornitori di disporre di un piano di prova in condizioni reali presentato all'autorità di vigilanza del mercato competente, di registrare le prove in sezioni dedicate della banca dati dell'UE, fatte salve alcune limitate eccezioni, di fissare limiti al periodo nel quale possono essere effettuate le prove e di richiedere tutele aggiuntive per le persone appartenenti a certi gruppi vulnerabili, nonché un accordo scritto che definisca i ruoli e le responsabilità dei potenziali fornitori e dei deployer e una sorveglianza efficace da parte del personale competente coinvolto nelle prove in condizioni reali. È inoltre opportuno prevedere tutele aggiuntive per garantire che le previsioni, le raccomandazioni o le decisioni del sistema di IA possano essere efficacemente ribaltate e ignorate e che i dati personali siano protetti e cancellati quando i soggetti hanno revocato il loro consenso a partecipare alle prove, fatti salvi i loro diritti in qualità di interessati ai sensi della normativa dell'Unione in materia di protezione dei dati. Per quanto riguarda il trasferimento dei dati, è inoltre opportuno prevedere che i dati raccolti e trattati ai fini delle prove in condizioni reali siano trasferiti a paesi terzi solo se sono attuate tutele adeguate e applicabili ai sensi del diritto dell'Unione, in particolare conformemente alle basi per il trasferimento di dati personali ai sensi del diritto dell'Unione in materia di protezione dei dati, mentre per i dati non personali sono poste in essere tutele adeguate conformemente al diritto dell'Unione, quali il regolamento (UE) 2022/868¹⁵⁸ e il regolamento (UE) 2023/2854¹⁵⁹ del Parlamento europeo e del Consiglio.

¹⁵⁸ Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla governance dei dati) (GU L 152 del 3.6.2022, pag. 1).

¹⁵⁹ Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati) (GU L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

(142) Per garantire che l'IA porti a risultati vantaggiosi sul piano sociale e ambientale, gli Stati membri sono incoraggiati a sostenere e promuovere la ricerca e lo sviluppo di soluzioni di IA a sostegno di risultati vantaggiosi dal punto di vista sociale e ambientale, come le soluzioni basate sull'IA per aumentare l'accessibilità per le persone con disabilità, affrontare le disuguaglianze socioeconomiche o conseguire obiettivi in materia di ambiente, assegnando risorse sufficienti, compresi i finanziamenti pubblici e dell'Unione, e, se del caso e a condizione che siano soddisfatti i criteri di ammissibilità e selezione, prendendo in considerazione soprattutto i progetti che perseguono tali obiettivi. Tali progetti dovrebbero basarsi sul principio della cooperazione interdisciplinare tra sviluppatori dell'IA, esperti in materia di disuguaglianza e non discriminazione, accessibilità e diritti ambientali, digitali e dei consumatori, nonché personalità accademiche.

(143) Al fine di promuovere e proteggere l'innovazione, è importante che siano tenuti in particolare considerazione gli interessi delle PMI, comprese le start-up, che sono fornitrici o deployer di sistemi di IA. È a tal fine opportuno che gli Stati membri sviluppino iniziative destinate a tali operatori, anche in materia di sensibilizzazione e comunicazione delle informazioni. Gli Stati membri dovrebbero fornire alle PMI, comprese le start-up, con sede legale o una filiale nell'Unione, un accesso prioritario agli spazi di sperimentazione normativa per l'IA, purché soddisfino le condizioni di ammissibilità e i criteri di selezione e senza precludere ad altri fornitori e potenziali fornitori l'accesso agli spazi di sperimentazione, a condizione che siano soddisfatti gli stessi criteri e le stesse condizioni. Gli Stati membri dovrebbero utilizzare i canali esistenti e, ove opportuno, istituiscono nuovi canali dedicati per la comunicazione con le PMI, comprese le start-up, i deployer, altri innovatori e, se del caso, le autorità pubbliche locali, al fine di sostenere le PMI nel loro percorso di sviluppo fornendo orientamenti e rispondendo alle domande sull'attuazione del presente regolamento. Se del caso, tali canali dovrebbero collaborare per creare sinergie e garantire l'omogeneità dei loro orientamenti per le PMI, comprese le start-up, e i deployer. Inoltre, gli Stati membri dovrebbero agevolare la partecipazione delle PMI e di altri portatori di interessi pertinenti ai processi di sviluppo della normazione. Gli organismi notificati, nel fissare le tariffe per la valutazione della conformità, dovrebbero tenere in considerazione gli interessi e le esigenze specifici dei fornitori che sono PMI, comprese le start-up. La Commissione dovrebbe valutare periodicamente i costi di certificazione e di conformità per le PMI, comprese le start-up, attraverso consultazioni trasparenti e dovrebbe collaborare con gli Stati membri per ridurre tali costi.

Ad esempio, le spese di traduzione connesse alla documentazione obbligatoria e alla comunicazione con le autorità possono rappresentare un costo significativo per i fornitori e gli altri operatori, in particolare quelli di dimensioni ridotte. Gli Stati membri dovrebbero garantire, se possibile, che una delle lingue da essi indicate e accettate per la documentazione dei fornitori pertinenti e per la comunicazione con gli operatori sia una lingua ampiamente compresa dal maggior numero possibile di deployer transfrontalieri. Al fine di rispondere alle esigenze specifiche delle PMI, comprese le start-up, la Commissione dovrebbe fornire modelli standardizzati per i settori disciplinati dal presente regolamento, su richiesta del consiglio per l'IA. Inoltre, la Commissione dovrebbe integrare gli sforzi degli Stati membri fornendo a tutti i fornitori e i deployer una piattaforma unica di informazioni di facile utilizzo in relazione al presente regolamento, organizzando adeguate campagne di comunicazione per sensibilizzare in merito agli obblighi derivanti dal presente regolamento e valutando e promuovendo la convergenza delle migliori pratiche nelle procedure di appalto pubblico in relazione ai sistemi di IA. Le imprese che di recente sono passate dalla categoria delle piccole imprese a quella delle medie imprese ai sensi dell'allegato della raccomandazione 2003/361/CE¹⁶⁰ della Commissione dovrebbero avere accesso a tali misure di sostegno, in quanto queste nuove imprese di medie dimensioni possono talvolta non disporre delle risorse giuridiche e della formazione necessarie per garantire una corretta comprensione del presente regolamento e la conformità ad esso.

¹⁶⁰ Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

- (144) Al fine di promuovere e proteggere l'innovazione, la piattaforma di IA on demand e tutti i pertinenti programmi e progetti di finanziamento dell'Unione, quali il programma Europa digitale e Orizzonte Europa, attuati dalla Commissione e dagli Stati membri a livello dell'Unione o nazionale, a seconda dei casi, dovrebbero contribuire al conseguimento degli obiettivi del presente regolamento.
- (145) Al fine di ridurre al minimo i rischi per l'attuazione derivanti dalla mancanza di conoscenze e competenze sul mercato, nonché per agevolare il rispetto, da parte dei fornitori, in particolare le PMI, comprese le start-up, e degli organismi notificati, degli obblighi loro imposti dal presente regolamento, è opportuno che la piattaforma di IA on demand, i poli europei dell'innovazione digitale e gli impianti di prova e sperimentazione istituiti dalla Commissione e dagli Stati membri a livello dell'Unione o nazionale contribuiscano all'attuazione del presente regolamento. Nell'ambito delle rispettive missioni e dei rispettivi settori di competenza, la piattaforma di IA on demand, i poli europei dell'innovazione digitale e gli impianti di prova e sperimentazione sono in grado di fornire, in particolare, sostegno tecnico e scientifico ai fornitori e agli organismi notificati.

- (146) Inoltre, alla luce delle dimensioni molto ridotte di alcuni operatori e al fine di garantire la proporzionalità rispetto ai costi dell'innovazione, è opportuno consentire alle microimprese di adempiere a uno degli obblighi più dispendiosi, vale a dire l'istituzione di un sistema di gestione della qualità, in un modo semplificato che ridurrebbe gli oneri amministrativi e i costi a carico di tali imprese senza incidere sul livello di protezione e sulla necessità di rispettare i requisiti per i sistemi di IA ad alto rischio. La Commissione dovrebbe elaborare orientamenti per specificare gli elementi del sistema di gestione della qualità che le microimprese devono soddisfare in tale modo semplificato.
- (147) È opportuno che la Commissione agevoli, nella misura del possibile, l'accesso agli impianti di prova e sperimentazione di organismi, gruppi o laboratori istituiti o accreditati a norma di qualsiasi pertinente normativa di armonizzazione dell'Unione che assolvono compiti nel contesto della valutazione della conformità di prodotti o dispositivi contemplati da tale normativa di armonizzazione dell'Unione. Ciò vale in particolare per quanto riguarda i gruppi di esperti, i laboratori specializzati e i laboratori di riferimento nel settore dei dispositivi medici a norma dei regolamenti (UE) 2017/745 e (UE) 2017/746.

(148) Il presente regolamento dovrebbe istituire un quadro di governance che consenta di coordinare e sostenere l'applicazione dello stesso a livello nazionale, nonché di sviluppare capacità a livello dell'Unione e integrare i portatori di interessi nel settore dell'IA. L'attuazione e l'esecuzione efficaci del presente regolamento richiedono un quadro di governance che consenta di coordinare e sviluppare competenze centrali a livello dell'Unione. L'ufficio per l'IA è stato istituito con decisione della Commissione¹⁶¹ e ha la missione di sviluppare competenze e capacità dell'Unione nel settore dell'IA e di contribuire all'attuazione del diritto dell'Unione in materia di IA. Gli Stati membri dovrebbero facilitare i compiti dell'ufficio per l'IA al fine di sostenere lo sviluppo di competenze e capacità dell'Unione a livello dell'Unione e di rafforzare il funzionamento del mercato unico digitale. È inoltre opportuno istituire un consiglio per l'IA composto da rappresentanti degli Stati membri, un gruppo di esperti scientifici volto a integrare la comunità scientifica e un forum consultivo per raccogliere il contributo dei portatori di interessi all'attuazione del presente regolamento, a livello dell'Unione e nazionale. Lo sviluppo delle competenze e delle capacità dell'Unione dovrebbe includere anche l'utilizzo delle risorse e delle competenze esistenti, in particolare grazie a sinergie con le strutture create nel contesto dell'esecuzione a livello dell'Unione di altre disposizioni e a sinergie con le iniziative correlate a livello dell'Unione, quali l'impresa comune EuroHPC e gli impianti di prova e sperimentazione dell'IA nell'ambito del programma Europa digitale.

¹⁶¹ Decisione della Commissione, del 24 gennaio 2024, che istituisce l'Ufficio europeo per l'intelligenza artificiale C (2024) 390.

(149) Al fine di facilitare un'attuazione agevole, efficace e armonizzata del presente regolamento, è opportuno istituire un consiglio per l'IA. Il consiglio per l'IA dovrebbe riflettere i vari interessi dell'ecosistema dell'IA ed essere composto da rappresentanti degli Stati membri. Il consiglio per l'IA dovrebbe essere responsabile di una serie di compiti consultivi, tra cui l'emanazione di pareri, raccomandazioni, consulenze o il contributo all'emanazione di orientamenti su questioni relative all'attuazione del presente regolamento, comprese le questioni relative all'esecuzione, le specifiche tecniche o le norme esistenti per quanto riguarda i requisiti stabiliti nel presente regolamento, e la fornitura di consulenza alla Commissione, agli Stati membri e alle rispettive autorità nazionali competenti su questioni specifiche connesse all'IA. Al fine di offrire una certa flessibilità agli Stati membri nella designazione dei loro rappresentanti all'interno del consiglio per l'IA, tali rappresentanti possono essere persone appartenenti a entità pubbliche dotate delle competenze e dei poteri pertinenti per facilitare il coordinamento a livello nazionale e contribuire all'adempimento dei compiti del consiglio per l'IA. Il consiglio per l'IA dovrebbe istituire due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e le autorità di notifica su questioni relative, rispettivamente, alla vigilanza del mercato e agli organismi notificati. Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per il presente regolamento ai sensi dell'articolo 30 del regolamento (UE) 2019/1020. In conformità dell'articolo 33 di tale regolamento, la Commissione dovrebbe sostenere le attività del sottogruppo permanente per la vigilanza del mercato effettuando valutazioni o studi di mercato, in particolare al fine di individuare gli aspetti del presente regolamento che richiedono un coordinamento specifico e urgente tra le autorità di vigilanza del mercato. Il consiglio per l'IA può istituire altri sottogruppi permanenti o temporanei, se del caso, ai fini dell'esame di questioni specifiche. Il consiglio per l'IA dovrebbe inoltre cooperare, se del caso, con i pertinenti organismi, gruppi di esperti e reti dell'Unione attivi nel contesto del pertinente diritto dell'Unione, compresi in particolare quelli attivi a norma del pertinente diritto dell'Unione sui dati, i prodotti e i servizi digitali.

- (150) Al fine di garantire il coinvolgimento dei portatori di interessi nell'attuazione e nell'applicazione del presente regolamento, è opportuno istituire un forum consultivo per fornire consulenza e competenze tecniche al consiglio per l'IA e alla Commissione. Al fine di garantire una rappresentanza diversificata ed equilibrata dei portatori di interessi che tenga conto di interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, con riferimento alle PMI e alle altre imprese, il forum consultivo dovrebbe comprendere, tra l'altro, l'industria, le start-up, le PMI, il mondo accademico, la società civile, comprese le parti sociali, nonché l'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo delle norme di telecomunicazione (ETSI).
- (151) Al fine di sostenere l'attuazione e l'esecuzione del presente regolamento, in particolare le attività di monitoraggio dell'ufficio per l'IA per quanto riguarda i modelli di IA per finalità generali, è opportuno istituire un gruppo di esperti scientifici indipendenti. Gli esperti indipendenti che costituiscono il gruppo dovrebbero essere selezionati sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'IA e dovrebbero svolgere i loro compiti con imparzialità e obiettività e garantire la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività. Per consentire il potenziamento delle capacità nazionali necessarie per l'efficace esecuzione del presente regolamento, gli Stati membri dovrebbero essere in grado di chiedere il sostegno della riserva di esperti che costituisce il gruppo di esperti scientifici per le loro attività di esecuzione.

- (152) Al fine di sostenere un'esecuzione adeguata per quanto riguarda i sistemi di IA e rafforzare le capacità degli Stati membri, è opportuno istituire e mettere a disposizione degli Stati membri strutture di sostegno dell'Unione per la prova dell'IA.
- (153) Gli Stati membri svolgono un ruolo chiave nell'applicare ed eseguire il presente regolamento. A tale riguardo, è opportuno che ciascuno Stato membro designi almeno una autorità di notifica e almeno una autorità di vigilanza del mercato come autorità nazionali competenti al fine di controllare l'applicazione e l'attuazione del presente regolamento. Gli Stati membri possono decidere di nominare qualsiasi tipo di entità pubblica per svolgere i compiti delle autorità nazionali competenti ai sensi del presente regolamento, conformemente alle loro specifiche caratteristiche ed esigenze organizzative nazionali. Al fine di incrementare l'efficienza organizzativa da parte degli Stati membri e di istituire un punto di contatto unico nei confronti del pubblico e di altre controparti sia a livello di Stati membri sia a livello di Unione, è opportuno che ciascuno Stato membro designi un'autorità di vigilanza del mercato come punto di contatto unico.
- (154) Le autorità nazionali competenti dovrebbero esercitare i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità dovrebbero astenersi da qualsiasi atto incompatibile con le loro funzioni e dovrebbero essere soggetti alle norme in materia di riservatezza ai sensi del presente regolamento.

- (155) Al fine di garantire che i fornitori di sistemi di IA ad alto rischio possano tenere in considerazione l'esperienza sull'uso di sistemi di IA ad alto rischio per migliorare i loro sistemi e il processo di progettazione e sviluppo o possano adottare tempestivamente eventuali misure correttive, è opportuno che tutti i fornitori dispongano di un sistema di monitoraggio successivo all'immissione sul mercato. Se del caso, il monitoraggio successivo all'immissione sul mercato dovrebbe includere un'analisi dell'interazione con altri sistemi di IA, compresi altri dispositivi e software. Il monitoraggio successivo all'immissione sul mercato non dovrebbe riguardare i dati operativi sensibili dei deployer che sono autorità di contrasto. Tale sistema è altresì fondamentale per garantire che i possibili rischi derivanti dai sistemi di IA che proseguono il loro "apprendimento" dopo essere stati immessi sul mercato o messi in servizio possano essere affrontati in modo più efficiente e tempestivo. I fornitori dovrebbero anche essere tenuti, in tale contesto, a predisporre un sistema per segnalare alle autorità competenti eventuali incidenti gravi derivanti dall'uso dei loro sistemi di IA, vale a dire incidenti o malfunzionamenti che comportano il decesso o gravi danni alla salute, perturbazioni gravi e irreversibili della gestione o del funzionamento delle infrastrutture critiche, violazioni degli obblighi ai sensi del diritto dell'Unione intesi a proteggere i diritti fondamentali o gravi danni alle cose o all'ambiente.

(156) Al fine di garantire un'esecuzione adeguata ed efficace dei requisiti e degli obblighi stabiliti dal presente regolamento, che costituisce la normativa di armonizzazione dell'Unione, è opportuno che si applichi nella sua interezza il sistema di vigilanza del mercato e di conformità dei prodotti istituito dal regolamento (UE) 2019/1020. Le autorità di vigilanza del mercato designate a norma del presente regolamento dovrebbero disporre di tutti i poteri di esecuzione di cui al presente regolamento e al regolamento (UE) 2019/1020 e dovrebbero esercitare i loro poteri e svolgere le loro funzioni in modo indipendente, imparziale e senza pregiudizi. Sebbene la maggior parte dei sistemi di IA non sia soggetta a requisiti e obblighi specifici a norma del presente regolamento, le autorità di vigilanza del mercato possono adottare misure in relazione a tutti i sistemi di IA che presentino un rischio conformemente al presente regolamento. Data la natura specifica delle istituzioni, degli organi e degli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento, è opportuno designare il Garante europeo della protezione dei dati quale autorità di vigilanza del mercato per essi competente. Ciò non dovrebbe pregiudicare la designazione di autorità nazionali competenti da parte degli Stati membri. Le attività di vigilanza del mercato non dovrebbero pregiudicare la capacità delle entità sottoposte a vigilanza di svolgere i loro compiti in modo indipendente, qualora tale indipendenza sia richiesta dal diritto dell'Unione.

(157) Il presente regolamento non pregiudica le competenze, i compiti, i poteri e l'indipendenza delle autorità o degli organismi pubblici nazionali competenti che controllano l'applicazione del diritto dell'Unione che tutela i diritti fondamentali, compresi gli organismi per la parità e le autorità per la protezione dei dati. Ove necessario per il loro mandato, è opportuno che tali autorità od organismi pubblici nazionali abbiano altresì accesso alla documentazione creata a norma del presente regolamento. È opportuno istituire una procedura di salvaguardia specifica per garantire un'esecuzione adeguata e tempestiva rispetto ai sistemi di IA che presentano un rischio per la salute, la sicurezza e i diritti fondamentali. La procedura per siffatti sistemi di IA che presentano un rischio dovrebbe essere applicata ai sistemi di IA ad alto rischio che presentano un rischio, ai sistemi vietati che sono stati immessi sul mercato, messi in servizio o utilizzati in violazione dei divieti riguardanti le pratiche di cui al presente regolamento e ai sistemi di IA che sono stati messi a disposizione in violazione dei requisiti di trasparenza di cui al presente regolamento e che presentano un rischio.

(158) Il diritto dell'Unione in materia di servizi finanziari comprende regole e requisiti in materia di governance interna e di gestione dei rischi che sono applicabili agli istituti finanziari regolamentati durante la fornitura di tali servizi, anche quando si avvalgono di sistemi di IA. Al fine di garantire la coerenza dell'applicazione e dell'esecuzione degli obblighi previsti dal presente regolamento e delle regole e dei requisiti pertinenti degli atti giuridici dell'Unione in materia di servizi finanziari, è opportuno che le autorità competenti del controllo e dell'esecuzione di tali atti giuridici, in particolare le autorità competenti quali definite al regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio¹⁶² e alle direttive 2008/48/CE¹⁶³, 2009/138/CE¹⁶⁴, 2013/36/UE¹⁶⁵, 2014/17/UE¹⁶⁶ e (UE) 2016/97¹⁶⁷ del Parlamento europeo e del Consiglio, siano designate, nell'ambito delle rispettive competenze, quali autorità competenti ai fini del controllo dell'attuazione del presente regolamento, anche in relazione alle attività di vigilanza del mercato, per quanto riguarda i sistemi di IA forniti o utilizzati da istituti finanziari regolamentati e sottoposti a vigilanza, a meno che gli Stati membri non decidano di designare un'altra autorità per svolgere tali compiti di vigilanza del mercato.

¹⁶² Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il regolamento (UE) n. 648/2012 (GU L 176 del 27.6.2013, pag. 1).

¹⁶³ 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE (GU L 133 del 22.5.2008, pag. 66).

¹⁶⁴ Direttiva 2009/138/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 in materia di accesso ed esercizio delle attività di assicurazione e di riassicurazione (solvibilità II) (GU L 335 del 17.12.2009, pag. 1).

¹⁶⁵ Direttiva 2013/36/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, sull'accesso all'attività degli enti creditizi e sulla vigilanza prudenziale sugli enti creditizi e sulle imprese di investimento, che modifica la direttiva 2002/87/CE e abroga le direttive 2006/48/CE e 2006/49/CE (GU L 176 del 27.6.2013, pag. 338).

¹⁶⁶ Direttiva 2014/17/UE del Parlamento europeo e del Consiglio, del 4 febbraio 2014, in merito ai contratti di credito ai consumatori relativi a beni immobili residenziali e recante modifica delle direttive 2008/48/CE e 2013/36/UE e del regolamento (UE) n. 1093/2010 (GU L 60 del 28.2.2014, pag. 34).

¹⁶⁷ Direttiva (UE) 2016/97 del Parlamento europeo e del Consiglio, del 20 gennaio 2016, sulla distribuzione assicurativa (GU L 26 del 2.2.2016, pag. 19).

Tali autorità competenti dovrebbero disporre di tutti i poteri a norma del presente regolamento e del regolamento (UE) 2019/1020 per far rispettare i requisiti e gli obblighi del presente regolamento, compresi i poteri per svolgere attività di vigilanza del mercato *ex post* che possono essere integrate, se del caso, nei rispettivi meccanismi e nelle rispettive procedure di vigilanza esistenti a norma del pertinente diritto dell'Unione in materia di servizi finanziari. È opportuno prevedere che, quando agiscono in qualità di autorità di vigilanza del mercato a norma del presente regolamento, le autorità nazionali responsabili della vigilanza degli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento (UE) n. 1024/2013 del Consiglio¹⁶⁸, comunichino senza ritardo alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento. Per migliorare ulteriormente la coerenza tra il presente regolamento e le regole applicabili agli enti creditizi disciplinati dalla direttiva 2013/36/UE, è altresì opportuno integrare negli obblighi e nelle procedure esistenti a norma di tale direttiva alcuni degli obblighi procedurali dei fornitori in materia di gestione dei rischi, monitoraggio successivo all'immissione sul mercato e documentazione. Al fine di evitare sovrapposizioni, è opportuno prevedere deroghe limitate anche in relazione al sistema di gestione della qualità dei fornitori e all'obbligo di monitoraggio imposto ai deployer dei sistemi di IA ad alto rischio nella misura in cui si applicano agli enti creditizi disciplinati dalla direttiva 2013/36/UE. Lo stesso regime dovrebbe applicarsi alle imprese di assicurazione e di riassicurazione e alle società di partecipazione assicurativa ai sensi della direttiva 2009/138/CE nonché agli intermediari assicurativi ai sensi della direttiva (UE) 2016/97 e ad altri tipi di istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del pertinente diritto dell'Unione in materia di servizi finanziari per garantire coerenza e parità di trattamento nel settore finanziario.

¹⁶⁸ Regolamento (UE) n. 1024/2013 del Consiglio, del 15 ottobre 2013, che attribuisce alla Banca centrale europea compiti specifici in merito alle politiche in materia di vigilanza prudenziale degli enti creditizi (GU L 287 del 29.10.2013, pag. 63).

- (159) Ciascuna autorità di vigilanza del mercato per i sistemi di IA ad alto rischio nel settore della biometria elencati in un allegato del presente regolamento nella misura in cui tali sistemi siano utilizzati a fini di contrasto, migrazione, asilo e gestione del controllo delle frontiere, o per l'amministrazione della giustizia e dei processi democratici, dovrebbe disporre di poteri di indagine e correttivi efficaci, tra cui almeno il potere di ottenere l'accesso a tutti i dati personali trattati e a tutte le informazioni necessarie per lo svolgimento dei suoi compiti. Le autorità di vigilanza del mercato dovrebbero poter esercitare i loro poteri agendo in piena indipendenza. Qualsiasi limitazione del loro accesso ai dati operativi sensibili a norma del presente regolamento dovrebbe lasciare impregiudicati i poteri loro conferiti dalla direttiva (UE) 2016/680. Nessuna esclusione relativa alla divulgazione dei dati alle autorità nazionali per la protezione dei dati a norma del presente regolamento dovrebbe incidere sui poteri attuali o futuri di tali autorità al di là dell'ambito di applicazione del presente regolamento.
- (160) Le autorità di vigilanza del mercato e la Commissione dovrebbero poter proporre attività congiunte, comprese indagini congiunte, che dovrebbero essere condotte dalle autorità di vigilanza del mercato o dalle autorità di vigilanza del mercato di concerto con la Commissione, al fine di promuovere la conformità, individuare casi di non conformità, sensibilizzare e fornire orientamenti in relazione al presente regolamento riguardo a specifiche categorie di sistemi di IA ad alto rischio che si rileva presentino un rischio grave in due o più Stati membri. Le attività congiunte volte a promuovere la conformità dovrebbero essere svolte conformemente all'articolo 9 del regolamento (UE) 2019/1020. L'ufficio per l'IA dovrebbe fornire sostegno di coordinamento per le indagini congiunte.

(161) È necessario chiarire le responsabilità e le competenze a livello dell'Unione e nazionale per quanto riguarda i sistemi di IA basati su modelli di IA per finalità generali. Per evitare sovrapposizioni di competenze, qualora un sistema di IA si basi su un modello di IA per finalità generali e il modello e il sistema siano forniti dallo stesso fornitore, la supervisione dovrebbe avere luogo a livello dell'Unione attraverso l'ufficio per l'IA, che dovrebbe disporre a tal fine dei poteri di un'autorità di vigilanza del mercato ai sensi del regolamento (UE) 2019/1020. In tutti gli altri casi, le autorità nazionali di vigilanza del mercato restano responsabili della supervisione dei sistemi di IA. Tuttavia, per i sistemi di IA per finalità generali che possono essere utilizzati direttamente dai deployer per almeno una finalità classificata come ad alto rischio, le autorità di vigilanza del mercato dovrebbero cooperare con l'ufficio per l'IA per effettuare valutazioni della conformità e informare di conseguenza il consiglio per l'IA e le altre autorità di vigilanza del mercato. Inoltre, qualsiasi autorità di vigilanza del mercato dovrebbero poter chiedere assistenza all'ufficio per l'IA qualora non sia in grado di concludere un'indagine su un sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali su cui è costruito il sistema di IA ad alto rischio. In tali casi, dovrebbe applicarsi mutatis mutandis la procedura relativa all'assistenza reciproca nei casi transfrontalieri di cui al capo VI del regolamento (UE) 2019/1020.

- (162) Per sfruttare al meglio le competenze centralizzate dell'Unione e le sinergie a livello dell'Unione, i poteri di controllo ed esecuzione degli obblighi dei fornitori di modelli di IA per finalità generali dovrebbero essere di competenza della Commissione. L'ufficio per l'IA dovrebbe essere in grado di svolgere tutte le attività necessarie per monitorare l'efficace attuazione del presente regolamento per quanto riguarda i modelli di IA per finalità generali. Dovrebbe essere in grado di svolgere indagini su eventuali violazioni delle norme applicabili ai fornitori di modelli di IA per finalità generali sia di propria iniziativa, a seguito dei risultati delle sue attività di monitoraggio, sia su richiesta delle autorità di vigilanza del mercato in linea con le condizioni stabilite nel presente regolamento. Per sostenere un monitoraggio efficace dell'ufficio per l'IA, esso dovrebbe prevedere la possibilità che i fornitori a valle presentino reclami in merito a possibili violazioni delle norme applicabili ai fornitori di modelli e sistemi di IA per finalità generali.
- (163) Al fine di integrare i sistemi di governance per i modelli di IA per finalità generali, il gruppo di esperti scientifici dovrebbe sostenere le attività di monitoraggio dell'ufficio per l'IA e può, in alcuni casi, fornire segnalazioni qualificate all'ufficio per l'IA che avviano attività di follow-up quali indagini. Ciò dovrebbe valere quando il gruppo di esperti scientifici ha motivo di sospettare che un modello di IA per finalità generali rappresenti un rischio concreto e identificabile a livello dell'Unione. Inoltre, ciò dovrebbe verificarsi nel caso in cui il gruppo di esperti scientifici abbia motivo di sospettare che un modello di IA per finalità generali soddisfa i criteri che comporterebbero una classificazione come modello di IA per finalità generali con rischio sistemico. Per dotare il gruppo di esperti scientifici delle informazioni necessarie per lo svolgimento di tali compiti, è opportuno prevedere un meccanismo in base al quale il gruppo di esperti scientifici può chiedere alla Commissione di esigere da un fornitore documentazione o informazioni.

- (164) L'ufficio per l'IA dovrebbe essere in grado di adottare le misure necessarie per monitorare l'efficace attuazione e il rispetto degli obblighi dei fornitori di modelli di IA per finalità generali di cui al presente regolamento. L'ufficio per l'IA dovrebbe essere in grado di svolgere indagini su possibili violazioni conformemente ai poteri previsti dal presente regolamento, anche richiedendo documentazione e informazioni, effettuando valutazioni ed esigendo l'adozione di misure da parte dei fornitori di modelli di IA per finalità generali. Nell'effettuare le valutazioni, al fine di avvalersi di competenze indipendenti, l'ufficio per l'IA dovrebbe potersi rivolgere a esperti indipendenti che svolgano le valutazioni per suo conto. Il rispetto degli obblighi dovrebbe essere reso esecutivo, tra l'altro, mediante richieste di adottare misure adeguate, comprese misure di attenuazione dei rischi nel caso di rischi sistemici individuati, nonché limitando la messa a disposizione sul mercato, ritirando o richiamando il modello. A titolo di salvaguardia, ove ciò sia necessario al di là dei diritti procedurali di cui al presente regolamento, i fornitori di modelli di IA per finalità generali dovrebbero godere dei diritti procedurali di cui all'articolo 18 del regolamento (UE) 2019/1020, che dovrebbero applicarsi *mutatis mutandis*, fatti salvi i diritti procedurali più specifici previsti dal presente regolamento.

(165) Lo sviluppo di sistemi di IA diversi dai sistemi di IA ad alto rischio in conformità dei requisiti del presente regolamento può portare a una più ampia adozione nell'Unione di un'IA etica e affidabile. I fornitori di sistemi di IA non ad alto rischio dovrebbero essere incoraggiati a creare codici di condotta, che includano meccanismi di governance connessi, volti a promuovere l'applicazione volontaria di alcuni o tutti i requisiti obbligatori applicabili ai sistemi di IA ad alto rischio, adattati in funzione della finalità prevista dei sistemi e del minor rischio connesso e tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore, come modelli e schede dati. I fornitori e, se del caso, i deployer di tutti i sistemi di IA, ad alto rischio o meno, e modelli di IA dovrebbero inoltre essere incoraggiati ad applicare su base volontaria requisiti supplementari relativi, ad esempio, agli elementi degli orientamenti etici dell'Unione per un'IA affidabile, alla sostenibilità ambientale, alle misure di alfabetizzazione in materia di IA, alla progettazione e allo sviluppo inclusivi e diversificati dei sistemi di IA, anche prestando attenzione alle persone vulnerabili e all'accessibilità per le persone con disabilità, la partecipazione dei portatori di interessi, con il coinvolgimento, se del caso, dei portatori di interessi pertinenti quali le organizzazioni imprenditoriali e della società civile, il mondo accademico, le organizzazioni di ricerca, i sindacati e le organizzazioni per la tutela dei consumatori nella progettazione e nello sviluppo dei sistemi di IA, e alla diversità dei gruppi di sviluppo, compreso l'equilibrio di genere. Per essere efficaci, i codici di condotta volontari dovrebbero basarsi su obiettivi chiari e indicatori chiave di prestazione che consentano di misurare il conseguimento di tali obiettivi. Essi dovrebbero inoltre essere elaborati in modo inclusivo, se del caso, con il coinvolgimento dei portatori di interessi pertinenti, quali le organizzazioni imprenditoriali e della società civile, il mondo accademico, le organizzazioni di ricerca, i sindacati e le organizzazioni per la tutela dei consumatori. La Commissione può elaborare iniziative, anche di natura settoriale, per agevolare la riduzione degli ostacoli tecnici che ostruiscono lo scambio transfrontaliero di dati per lo sviluppo dell'IA, anche per quanto riguarda l'infrastruttura di accesso ai dati e l'interoperabilità semantica e tecnica dei diversi tipi di dati.

- (166) È importante che i sistemi di IA collegati a prodotti che non sono ad alto rischio in conformità del presente regolamento e che pertanto non sono tenuti a rispettare i requisiti stabiliti per i sistemi di IA ad alto rischio siano comunque sicuri al momento dell'immissione sul mercato o della messa in servizio. Per contribuire a tale obiettivo, sarebbe opportuno applicare come rete di sicurezza il regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio¹⁶⁹.
- (167) Al fine di garantire una cooperazione affidabile e costruttiva delle autorità competenti a livello dell'Unione e nazionale, è opportuno che tutte le parti coinvolte nell'applicazione del presente regolamento rispettino la riservatezza delle informazioni e dei dati ottenuti nell'assolvimento dei loro compiti, in conformità del diritto dell'Unione o nazionale. Dovrebbero svolgere i loro compiti e le loro attività in modo da proteggere, in particolare, i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali, l'efficace attuazione del presente regolamento, gli interessi pubblici e di sicurezza nazionale, l'integrità del procedimento penale o amministrativo e l'integrità delle informazioni classificate.

¹⁶⁹ Regolamento (UE) 2023/988 del Parlamento europeo e del Consiglio, del 10 maggio 2023, relativo alla sicurezza generale dei prodotti, che modifica il regolamento (UE) n. 1025/2012 del Parlamento europeo e del Consiglio e la direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, e che abroga la direttiva 2001/95/CE del Parlamento europeo e del Consiglio e la direttiva 87/357/CEE del Consiglio (GU L 135 del 23.5.2023, pag. 1).

- (168) Il rispetto del presente regolamento dovrebbe essere reso esecutivo mediante l'imposizione di sanzioni e di altre misure di esecuzione. Gli Stati membri dovrebbero adottare tutte le misure necessarie per assicurare l'attuazione delle disposizioni di cui al presente regolamento, anche stabilendo sanzioni effettive, proporzionate e dissuasive in caso di violazione, anche nel rispetto del principio *ne bis in idem*. Al fine di rafforzare e armonizzare le sanzioni amministrative in caso di violazione del presente regolamento, è opportuno stabilire limiti massimi per la fissazione delle sanzioni amministrative pecuniarie per talune violazioni specifiche. Nel valutare l'importo delle sanzioni amministrative pecuniarie, gli Stati membri dovrebbero, in ogni singolo caso, tenere conto di tutte le circostanze pertinenti della situazione specifica, in particolare, della natura, della gravità e della durata della violazione e delle sue conseguenze e delle dimensioni del fornitore, in particolare se si tratta di una PMI, compresa una start-up. Il Garante europeo della protezione dei dati dovrebbe disporre del potere di infliggere sanzioni pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento.
- (169) Il rispetto degli obblighi imposti ai fornitori di modelli di IA per finalità generali a norma del presente regolamento dovrebbe essere reso esecutivo, tra l'altro, mediante sanzioni pecuniarie. A tal fine è opportuno stabilire livelli adeguati di sanzioni pecuniarie anche in caso di violazione di tali obblighi, tra cui il mancato rispetto delle misure richieste dalla Commissione a norma del presente regolamento, fatti salvi adeguati termini di prescrizione conformemente al principio di proporzionalità. Tutte le decisioni prese dalla Commissione a norma del presente regolamento sono soggette al controllo della Corte di giustizia dell'Unione europea conformemente al TFUE, compresa la giurisdizione, anche di merito, della Corte di giustizia riguardo alle sanzioni ai sensi dell'articolo 261 TFUE

- (170) Il diritto dell'Unione e nazionale prevedono già mezzi di ricorso efficaci per le persone fisiche e giuridiche sui cui diritti e sulle cui libertà incide negativamente l'uso dei sistemi di IA. Fatti salvi tali mezzi di ricorso, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione del presente regolamento dovrebbe avere il diritto di presentare un reclamo alla pertinente autorità di vigilanza del mercato.
- (171) Le persone interessate dovrebbero avere il diritto di ottenere una spiegazione qualora la decisione di un deployer si basi principalmente sugli output di determinati sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento e qualora tale decisione produca effetti giuridici o in modo analogo incida significativamente su tali persone in un modo che esse ritengano avere un impatto negativo sulla loro salute, sicurezza o sui loro diritti fondamentali. Tale spiegazione dovrebbe essere chiara e significativa e fornire una base su cui le persone interessate possano esercitare i loro diritti. Il diritto di ottenere una spiegazione non dovrebbe applicarsi all'uso di sistemi di IA per i quali il diritto dell'Unione o nazionale prevede eccezioni o restrizioni e dovrebbe applicarsi solo nella misura in cui tale diritto non sia già previsto dal diritto dell'Unione.
- (172) Le persone che agiscono in qualità di informatori in merito alle violazioni del presente regolamento dovrebbero essere protette a norma del diritto dell'Unione. La direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio¹⁷⁰ dovrebbe pertanto applicarsi alla segnalazione di violazioni del presente regolamento e alla protezione delle persone che segnalano tali violazioni.

¹⁷⁰ Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (GU L 305 del 26.11.2019, pag. 17).

(173) Al fine di garantire che il quadro normativo possa essere adeguato ove necessario, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per modificare le condizioni alle quali un sistema di IA non dovrebbe essere considerato ad alto rischio, l'elenco dei sistemi di IA ad alto rischio, le disposizioni relative alla documentazione tecnica, il contenuto della dichiarazione di conformità UE, le disposizioni relative alle procedure di valutazione della conformità, le disposizioni che stabiliscono i sistemi di IA ad alto rischio cui dovrebbe applicarsi la procedura di valutazione della conformità sulla base della valutazione del sistema di gestione della qualità e della valutazione della documentazione tecnica, la soglia, i parametri di riferimento e gli indicatori, anche integrando tali parametri di riferimento e indicatori, nelle regole per la classificazione di un modello di IA per finalità generali con rischio sistemico, i criteri per la designazione dei modelli di IA per finalità generali con rischio sistemico, la documentazione tecnica per i fornitori di modelli di IA per finalità generali e le informazioni sulla trasparenza per i fornitori di modelli di IA per finalità generali. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016¹⁷¹. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

¹⁷¹ GU L 123 del 12.5.2016, pag. 1.

(174) Dati i rapidi sviluppi tecnologici e le competenze tecniche necessarie per l'efficace applicazione del presente regolamento, la Commissione dovrebbe valutare e riesaminare il presente regolamento entro ... [cinque anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni quattro anni e presentare una relazione al Parlamento europeo e al Consiglio. Inoltre, tenuto conto delle implicazioni per l'ambito di applicazione del presente regolamento, la Commissione dovrebbe effettuare, una volta all'anno, una valutazione della necessità di modificare l'elenco dei sistemi di IA ad alto rischio e l'elenco delle pratiche vietate. Inoltre, entro ... [quattro anni dall'entrata in vigore del presente regolamento] e successivamente ogni quattro anni, la Commissione dovrebbe valutare la necessità di modificare l'elenco delle rubriche dei settori ad alto rischio di cui all'allegato del presente regolamento, i sistemi di IA che rientrano nell'ambito di applicazione degli obblighi di trasparenza, l'efficacia del sistema di supervisione e governance e i progressi compiuti riguardo allo sviluppo di prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico di modelli di IA per finalità generali, compresa la necessità di ulteriori misure o azioni, e riferire al Parlamento europeo e al Consiglio in merito. Entro il ... [quattro anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni tre anni la Commissione dovrebbe valutare l'impatto e l'efficacia dei codici di condotta volontari per la promozione dell'applicazione dei requisiti previsti per i sistemi di IA ad alto rischio nel caso di sistemi di IA diversi dai sistemi di IA ad alto rischio ed eventualmente di altri requisiti supplementari per tali sistemi di IA.

- (175) È opportuno attribuire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di esecuzione del presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio¹⁷².
- (176) Poiché l'obiettivo del presente regolamento, vale a dire migliorare il funzionamento del mercato interno e promuovere la diffusione di un'IA antropocentrica e affidabile, garantendo nel contempo un elevato livello di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione e promuovendo l'innovazione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata o degli effetti dell'azione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 TUE. Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

¹⁷² Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

- (177) Al fine di garantire la certezza del diritto, assicurare un adeguato periodo di adattamento per gli operatori ed evitare perturbazioni del mercato, anche garantendo la continuità dell'uso dei sistemi di IA, è opportuno che il presente regolamento si applichi ai sistemi di IA ad alto rischio che sono stati immessi sul mercato o messi in servizio prima della data generale di applicazione dello stesso, solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione o finalità prevista. È opportuno precisare che, a tale riguardo, il concetto di modifica significativa dovrebbe essere inteso come equivalente nella sostanza alla nozione di modifica sostanziale, utilizzata solo per i sistemi di IA ad alto rischio a norma del presente regolamento. In via eccezionale e alla luce della responsabilità pubblica, gli operatori di sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati in un allegato del presente regolamento e gli operatori di sistemi di IA ad alto rischio destinati a essere utilizzati dalle autorità pubbliche dovrebbero adottare le misure necessarie per conformarsi ai requisiti del presente regolamento, rispettivamente, entro la fine del 2030 ed entro ... [sei anni dalla data di entrata in vigore del presente regolamento].
- (178) I fornitori di sistemi di IA ad alto rischio sono incoraggiati a iniziare a rispettare, su base volontaria, i pertinenti obblighi del presente regolamento già durante il periodo transitorio.

(179) Il presente regolamento si dovrebbe applicare a decorrere dal ... [due anni dopo l'entrata in vigore del presente regolamento]. Tuttavia, tenuto conto del rischio inaccettabile associato all'uso dell'IA in determinati modi, i divieti nonché le disposizioni generali del presente regolamento dovrebbero applicarsi già a decorrere dal... [sei mesi dalla data di entrata in vigore del presente regolamento]. Sebbene la piena efficacia di tali divieti discenda dall'istituzione della governance e dall'esecuzione del presente regolamento, è importante anticipare l'applicazione di detti divieti per tenere conto dei rischi inaccettabili e avere un effetto su altre procedure, ad esempio nel diritto civile. È inoltre opportuno che l'infrastruttura relativa alla governance e al sistema di valutazione della conformità sia operativa prima del ... [due anni dalla data di entrata in vigore del presente regolamento], pertanto le disposizioni sugli organismi notificati e sulla struttura di governance dovrebbero applicarsi a decorrere dal... [12 mesi dalla data di entrata in vigore del presente regolamento]. In considerazione del rapido ritmo dello sviluppo tecnologico e dell'adozione di modelli di IA per finalità generali, gli obblighi per i fornitori di modelli di IA per finalità generali dovrebbero applicarsi a decorrere dal ... [12 mesi dalla data di entrata in vigore del presente regolamento]. I codici di buone pratiche dovrebbero essere pronti entro ... [nove mesi dalla data di entrata in vigore del presente regolamento] al fine di consentire ai fornitori di dimostrare la conformità "in tempo utile". L'ufficio per l'IA dovrebbe garantire che le norme e le procedure di classificazione siano aggiornate alla luce degli sviluppi tecnologici. Gli Stati membri dovrebbero inoltre stabilire e notificare alla Commissione la normativa relativa alle sanzioni, comprese le sanzioni amministrative pecuniarie, e garantire che essa sia attuata in modo corretto ed efficace entro la data di applicazione del presente regolamento. Le disposizioni relative alle sanzioni dovrebbero pertanto applicarsi a decorrere dal ... [12 mesi dopo l'entrata in vigore del presente regolamento].

- (180) Conformemente all'articolo 42, paragrafi 1 e 2, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati e il comitato europeo per la protezione dei dati sono stati consultati e hanno formulato il loro parere congiunto il 18 giugno 2021.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I

Disposizioni generali

Articolo 1

Oggetto

1. Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione.
2. Il presente regolamento stabilisce:
 - a) regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione;
 - b) divieti di talune pratiche di IA;
 - c) requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi;
 - d) regole di trasparenza armonizzate per determinati sistemi di IA;
 - e) regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali;

- f) regole in materia di monitoraggio del mercato, vigilanza del mercato, governance ed esecuzione;
- g) misure a sostegno dell'innovazione, con particolare attenzione alle PMI, comprese le start-up.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica:

- a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo;
- b) ai deployer dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione;
- c) ai fornitori e ai deployer di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione;
- d) agli importatori e ai distributori di sistemi di IA;
- e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio;
- f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione;
- g) alle persone interessate che si trovano nell'Unione.

2. Ai sistemi di IA classificati come ad alto rischio ai sensi dell'articolo 6, paragrafo 1, relativo a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione B, si applicano unicamente l'articolo 6, paragrafo 1, gli articoli da 102 a 109 e l'articolo 112. L'articolo 57 si applica solo nella misura in cui i requisiti per i sistemi di IA ad alto rischio a norma del presente regolamento siano stati integrati in tale normativa di armonizzazione dell'Unione.
3. Il presente regolamento non si applica a settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudica le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze.

Il presente regolamento non si applica ai sistemi di IA se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

Il presente regolamento non si applica ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

4. Il presente regolamento non si applica alle autorità pubbliche di un paese terzo né alle organizzazioni internazionali che rientrano nell'ambito di applicazione del presente regolamento a norma del paragrafo 1, laddove tali autorità o organizzazioni utilizzino i sistemi di IA nel quadro della cooperazione o di accordi internazionali per la cooperazione delle autorità di contrasto e giudiziarie con l'Unione o con uno o più Stati membri, a condizione che tale paese terzo o organizzazione internazionale fornisca garanzie adeguate per quanto riguarda la protezione dei diritti e delle libertà fondamentali delle persone.
5. Il presente regolamento non pregiudica l'applicazione delle disposizioni sulla responsabilità dei prestatori di servizi intermediari di cui al capo II del regolamento (UE) 2022/2065.
6. Il presente regolamento non si applica ai sistemi di IA o modelli di IA, ivi compresi i loro output, specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici.
7. Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento.
8. Il presente regolamento non si applica alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio. Tali attività sono svolte in conformità del diritto dell'Unione applicabile. Le prove in condizioni reali non rientrano in tale esclusione.

9. Il presente regolamento lascia impregiudicate le norme stabilite da altri atti giuridici dell'Unione in materia di protezione dei consumatori e di sicurezza dei prodotti.
10. Il presente regolamento non si applica agli obblighi dei deployer che sono persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale.
11. Il presente regolamento non osta a che l'Unione o gli Stati membri mantengano o introducano disposizioni legislative, regolamentari o amministrative più favorevoli ai lavoratori in termini di tutela dei loro diritti in relazione all'uso dei sistemi di IA da parte dei datori di lavoro, o incoraggino o consentano l'applicazione di contratti collettivi più favorevoli ai lavoratori.
12. Il presente regolamento non si applica ai sistemi di IA rilasciati con licenza libera e open source, a meno che non siano immessi sul mercato o messi in servizio come sistemi di IA ad alto rischio o come sistema di IA rientrante nell'ambito di applicazione dell'articolo 5 o 50.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

- 1) "sistema di IA": un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

- 2) "rischio": la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso;
- 3) "fornitore": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito;
- 4) "deployer": una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale;
- 5) "rappresentante autorizzato": una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento;
- 6) "importatore": una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo;
- 7) "distributore": una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione;
- 8) "operatore": un fornitore, un fabbricante del prodotto, un deployer, un rappresentante autorizzato, un importatore o un distributore;

- 9) "immissione sul mercato": la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione;
- 10) "messa a disposizione sul mercato": la fornitura di un sistema di IA o di un modello di IA per finalità generali per la distribuzione o l'uso sul mercato dell'Unione nel corso di un'attività commerciale, a titolo oneroso o gratuito;
- 11) "messa in servizio": la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista;
- 12) "finalità prevista": l'uso di un sistema di IA previsto dal fornitore, compresi il contesto e le condizioni d'uso specifici, come dettagliati nelle informazioni comunicate dal fornitore nelle istruzioni per l'uso, nel materiale promozionale o di vendita e nelle dichiarazioni, nonché nella documentazione tecnica;
- 13) "uso improprio ragionevolmente prevedibile": l'uso di un sistema di IA in un modo non conforme alla sua finalità prevista, ma che può derivare da un comportamento umano o da un'interazione con altri sistemi, ivi compresi altri sistemi di IA, ragionevolmente prevedibile;
- 14) "componente di sicurezza": un componente di un prodotto o di un sistema di IA che svolge una funzione di sicurezza per tale prodotto o sistema di IA o il cui guasto o malfunzionamento mette in pericolo la salute e la sicurezza di persone o beni;
- 15) "istruzioni per l'uso": le informazioni comunicate dal fornitore per informare il deployer in particolare della finalità prevista e dell'uso corretto di un sistema di IA;

- 16) "richiamo di un sistema di IA": qualsiasi misura volta a ottenere la restituzione al fornitore, la messa fuori servizio o la disabilitazione dell'uso di un sistema di IA messo a disposizione dei deployer;
- 17) "ritiro di un sistema di IA": qualsiasi misura volta a impedire che un sistema di IA nella catena di approvvigionamento sia messo a disposizione sul mercato;
- 18) "prestazioni di un sistema di IA": la capacità di un sistema di IA di conseguire la finalità prevista;
- 19) "autorità di notifica": l'autorità nazionale responsabile dell'istituzione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio;
- 20) "valutazione della conformità": la procedura atta a dimostrare se i requisiti di cui al capo III, sezione 2, relativi a un sistema di IA ad alto rischio sono stati soddisfatti;
- 21) "organismo di valutazione della conformità": un organismo che svolge per conto di terzi attività di valutazione della conformità, incluse prove, certificazioni e ispezioni;
- 22) "organismo notificato": un organismo di valutazione della conformità notificato in conformità del presente regolamento e di altre pertinenti normative di armonizzazione dell'Unione;
- 23) "modifica sostanziale": una modifica di un sistema di IA a seguito della sua immissione sul mercato o messa in servizio che non è prevista o programmata nella valutazione iniziale della conformità effettuata dal fornitore e che ha l'effetto di incidere sulla conformità del sistema di IA ai requisiti di cui al capo III, sezione 2, o comporta una modifica della finalità prevista per la quale il sistema di IA è stato valutato;

- 24) "marcatura CE": una marcatura mediante la quale un fornitore indica che un sistema di IA è conforme ai requisiti stabiliti al capo III, sezione 2, e in altre normative di armonizzazione dell'Unione applicabili e che ne prevedono l'apposizione;
- 25) "sistema di monitoraggio successivo all'immissione sul mercato": tutte le attività svolte dai fornitori di sistemi di IA al fine di raccogliere e analizzare l'esperienza maturata tramite l'uso dei sistemi di IA che immettono sul mercato o che mettono in servizio, al fine di individuare eventuali necessità di immediate azioni correttive o preventive;
- 26) "autorità di vigilanza del mercato": l'autorità nazionale che svolge le attività e adotta le misure a norma del regolamento (UE) 2019/1020;
- 27) "norma armonizzata": la norma armonizzata di cui all'articolo 2, punto 1), lettera c), del regolamento (UE) n. 1025/2012;
- 28) "specifiche comuni": un insieme di specifiche tecniche quali definite all'articolo 2, punto 4), del regolamento (UE) n. 1025/2012, che forniscono i mezzi per soddisfare determinati requisiti stabiliti a norma del presente regolamento;
- 29) "dati di addestramento": i dati utilizzati per addestrare un sistema di IA adattandone i parametri che può apprendere;
- 30) "dati di convalida": i dati utilizzati per fornire una valutazione del sistema di IA addestrato e per metterne a punto, tra l'altro, i parametri che non può apprendere e il processo di apprendimento, al fine tra l'altro di evitare lo scarso (underfitting) o l'eccessivo (overfitting) adattamento ai dati di addestramento;

- 31) "set di dati di convalida": un set di dati distinto o costituito da una partizione fissa o variabile del set di dati di addestramento;
- 32) "dati di prova": i dati utilizzati per fornire una valutazione indipendente del sistema di IA al fine di confermarne le prestazioni attese prima della sua immissione sul mercato o messa in servizio;
- 33) "dati di input": i dati forniti a un sistema di IA o direttamente acquisiti dallo stesso, in base ai quali il sistema produce un output;
- 34) "dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, quali le immagini facciali o i dati dattiloscopici;
- 35) "identificazione biometrica": il riconoscimento automatizzato delle caratteristiche umane fisiche, fisiologiche, comportamentali o psicologiche allo scopo di determinare l'identità di una persona fisica confrontando i suoi dati biometrici con quelli di individui memorizzati in una banca dati;
- 36) "verifica biometrica": la verifica automatizzata e uno a uno, inclusa l'autenticazione, dell'identità di persone fisiche mediante il confronto dei loro dati biometrici con i dati biometrici forniti in precedenza;
- 37) "categorie particolari di dati personali": le categorie di dati personali di cui all'articolo 9, paragrafo 1, del regolamento (UE) 2016/679, all'articolo 10 della direttiva (UE) 2016/680 e all'articolo 10, paragrafo 1, del regolamento (UE) 2018/1725;

- 38) "dati operativi sensibili": dati operativi relativi ad attività di prevenzione, accertamento, indagine o perseguimento di reati, la cui divulgazione potrebbe compromettere l'integrità dei procedimenti penali;
- 39) "sistema di riconoscimento delle emozioni": un sistema di IA finalizzato all'identificazione o all'inferenza di emozioni o intenzioni di persone fisiche sulla base dei loro dati biometrici;
- 40) "sistema di categorizzazione biometrica": un sistema di IA che utilizza i dati biometrici di persone fisiche al fine di assegnarle a categorie specifiche, a meno che non sia accessorio a un altro servizio commerciale e strettamente necessario per ragioni tecniche oggettive;
- 41) "sistema di identificazione biometrica remota": un sistema di IA finalizzato all'identificazione di persone fisiche, senza il loro coinvolgimento attivo, tipicamente a distanza mediante il confronto dei dati biometrici di una persona con i dati biometrici contenuti in una banca dati di riferimento;
- 42) "sistema di identificazione biometrica remota "in tempo reale"": un sistema di identificazione biometrica remota in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono senza ritardi significativi, il quale comprende non solo le identificazioni istantanee, ma anche quelle che avvengono con brevi ritardi limitati al fine di evitare l'elusione;
- 43) "sistema di identificazione biometrica remota a posteriori": un sistema di identificazione biometrica remota diverso da un sistema di identificazione biometrica remota "in tempo reale";

- 44) "spazio accessibile al pubblico": qualsiasi luogo fisico di proprietà pubblica o privata accessibile a un numero indeterminato di persone fisiche, indipendentemente dal fatto che possano applicarsi determinate condizioni di accesso e indipendentemente dalle potenziali restrizioni di capacità;
- 45) "autorità di contrasto":
- a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse; oppure
 - b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;
- 46) "attività di contrasto": le attività svolte dalle autorità di contrasto o per loro conto a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse;
- 47) "ufficio per l'IA": la funzione della Commissione volta a contribuire all'attuazione, al monitoraggio e alla supervisione dei sistemi di IA e dei modelli di IA per finalità generali, e della governance dell'IA prevista dalla decisione della Commissione del 24 gennaio 2024. I riferimenti all'ufficio per l'IA contenuti nel presente regolamento si intendono fatti alla Commissione;

- 48) "autorità nazionale competente": un'autorità di notifica o un'autorità di vigilanza del mercato; per quanto riguarda i sistemi di IA messi in servizio o utilizzati da istituzioni, organi e organismi dell'Unione, i riferimenti alle autorità nazionali competenti o alle autorità di vigilanza del mercato contenuti nel presente regolamento si intendono fatti al Garante europeo della protezione dei dati;
- 49) "incidente grave": un incidente o malfunzionamento di un sistema di IA che, direttamente o indirettamente, causa una delle conseguenze seguenti:
- a) il decesso di una persona o gravi danni alla salute di una persona;
 - b) una perturbazione grave e irreversibile della gestione o del funzionamento delle infrastrutture critiche;
 - c) la violazione degli obblighi a norma del diritto dell'Unione intesi a proteggere i diritti fondamentali;
 - d) gravi danni alle cose o all'ambiente;
- 50) "dati personali": i dati personali quali definiti all'articolo 4, punto 1), del regolamento (UE) 2016/679;
- 51) "dati non personali": dati diversi dai dati personali di cui all'articolo 4, punto 1), del regolamento (UE) 2016/679;
- 52) "profilazione": la profilazione quale definita all'articolo 4, punto 4), del regolamento (UE) 2016/679;

- 53) "piano di prova in condizioni reali": un documento che descrive gli obiettivi, la metodologia, l'ambito geografico, della popolazione e temporale, il monitoraggio, l'organizzazione e lo svolgimento della prova in condizioni reali;
- 54) "piano dello spazio di sperimentazione": un documento concordato tra il fornitore partecipante e l'autorità competente in cui sono descritti gli obiettivi, le condizioni, il calendario, la metodologia e i requisiti relativamente alle attività svolte all'interno dello spazio di sperimentazione;
- 55) "spazio di sperimentazione normativa per l'IA": un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare;
- 56) "alfabetizzazione in materia di IA": le competenze, le conoscenze e la comprensione che consentono ai fornitori, ai deployer e alle persone interessate, tenendo conto dei loro rispettivi diritti e obblighi nel contesto del presente regolamento, di procedere a una diffusione informata dei sistemi di IA, nonché di acquisire consapevolezza in merito alle opportunità e ai rischi dell'IA e ai possibili danni che essa può causare;
- 57) "prova in condizioni reali": la prova temporanea di un sistema di IA per la sua finalità prevista in condizioni reali al di fuori di un laboratorio o di un ambiente altrimenti simulato al fine di raccogliere dati affidabili e solidi e di valutare e verificare la conformità del sistema di IA ai requisiti del presente regolamento e che non è considerata immissione sul mercato o messa in servizio del sistema di IA ai sensi del presente regolamento, purché siano soddisfatte tutte le condizioni di cui all'articolo 57 o 60;

- 58) "soggetto": ai fini della prova in condizioni reali, una persona fisica che partecipa a prove in condizioni reali;
- 59) "consenso informato": l'espressione libera, specifica, inequivocabile e volontaria di un soggetto della propria disponibilità a partecipare a una determinata prova in condizioni reali, dopo essere stato informato di tutti gli aspetti della prova rilevanti per la sua decisione di partecipare;
- 60) "deep fake": un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona;
- 61) "infrazione diffusa": qualsiasi azione od omissione contraria al diritto dell'Unione che tutela gli interessi delle persone:
- a) che abbia arrecato o possa arrecare un danno agli interessi collettivi di persone che risiedono in almeno due Stati membri diversi dallo Stato membro in cui:
 - i) ha avuto origine o si è verificato l'azione o l'omissione in questione;
 - ii) è ubicato o stabilito il fornitore interessato o, se del caso, il suo rappresentante autorizzato; oppure
 - iii) è stabilito il deployer, quando la violazione è commessa dal deployer;

- b) che abbia arrecato, arrechi o possa arrecare un danno agli interessi collettivi di persone e che presenti caratteristiche comuni, compresa la stessa pratica illecita e lo stesso interesse leso e che si verifichi simultaneamente, commessa dal medesimo operatore, in almeno tre Stati membri;
- 62) "infrastruttura critica": infrastruttura critica quale definita all'articolo 2, punto 4), della direttiva (UE) 2022/2557;
- 63) "modello di IA per finalità generali": un modello di IA, anche laddove tale modello di IA sia addestrato con grandi quantità di dati utilizzando l'autosupervisione su larga scala, che sia caratterizzato da una generalità significativa e sia in grado di svolgere con competenza un'ampia gamma di compiti distinti, indipendentemente dalle modalità con cui il modello è immesso sul mercato, e che può essere integrato in una varietà di sistemi o applicazioni a valle, ad eccezione dei modelli di IA utilizzati per attività di ricerca, sviluppo o prototipazione prima di essere immessi sul mercato;
- 64) "capacità di impatto elevato": capacità che corrispondono o superano le capacità registrate nei modelli di IA per finalità generali più avanzati;
- 65) "rischio sistemico": un rischio specifico per le capacità di impatto elevato dei modelli di IA per finalità generali, avente un impatto significativo sul mercato dell'Unione a causa della sua portata o di effetti negativi effettivi o ragionevolmente prevedibili sulla salute pubblica, la sicurezza, i diritti fondamentali o la società nel suo complesso, che può propagarsi su larga scala lungo l'intera catena del valore;

- 66) "sistema di IA per finalità generali": un sistema di IA basato su un modello di IA per finalità generali e che ha la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA;
- 67) "operazione in virgola mobile": qualsiasi operazione o assegnazione matematica che comporta numeri in virgola mobile, un sottoinsieme dei numeri reali generalmente rappresentati sui computer mediante un numero intero con precisione fissa avente come fattore di scala un esponente intero di una base fissa;
- 68) "fornitore a valle": un fornitore di un sistema di IA, compreso un sistema di IA per finalità generali, che integra un modello di IA, indipendentemente dal fatto che il modello di IA sia fornito dallo stesso e integrato verticalmente o fornito da un'altra entità sulla base di relazioni contrattuali.

Articolo 4

Alfabetizzazione in materia di IA

I fornitori e i deployer dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati.

Capo II

Pratiche di IA vietate

Articolo 5

Pratiche di IA vietate

1. Sono vietate le pratiche di IA seguenti:
 - a) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che utilizza tecniche subliminali che agiscono senza che una persona ne sia consapevole o tecniche volutamente manipolative o ingannevoli aventi lo scopo o l'effetto di distorcere materialmente il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la loro capacità di prendere una decisione informata, inducendole pertanto a prendere una decisione che non avrebbero altrimenti preso, in un modo che provochi o possa ragionevolmente provocare a tale persona, a un'altra persona o a un gruppo di persone un danno significativo;
 - b) l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla disabilità o a una specifica situazione sociale o economica, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno significativo;

- c) l'immissione sul mercato, la messa in servizio o l'uso di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti il verificarsi di uno o di entrambi gli scenari seguenti:
- i) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti;
 - ii) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;
- d) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di un sistema di IA per effettuare valutazioni del rischio relative a persone fisiche al fine di valutare o prevedere il rischio che una persona fisica commetta un reato, unicamente sulla base della profilazione di una persona fisica o della valutazione dei tratti e delle caratteristiche della personalità; tale divieto non si applica ai sistemi di IA utilizzati a sostegno della valutazione umana del coinvolgimento di una persona in un'attività criminosa, che si basa già su fatti oggettivi e verificabili direttamente connessi a un'attività criminosa;
- e) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA che creano o ampliano le banche dati di riconoscimento facciale mediante scraping non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;

- f) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, tranne laddove l'uso del sistema di IA sia destinato a essere messo in funzione o immesso sul mercato per motivi medici o di sicurezza;
- g) l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale; tale divieto non riguarda l'etichettatura o il filtraggio di set di dati biometrici acquisiti legalmente, come le immagini, sulla base di dati biometrici o della categorizzazione di dati biometrici nel settore delle attività di contrasto;
- h) l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti:
 - i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse;
 - ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico;

- iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni.

La lettera h) del primo comma lascia impregiudicato l'articolo 9 del regolamento (UE) 2016/679 per quanto riguarda il trattamento dei dati biometrici a fini diversi dall'attività di contrasto.

- 2. L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), è applicato ai fini di cui a tale lettera, solo per confermare l'identità della persona specificamente interessata e tiene conto degli elementi seguenti:
 - a) la natura della situazione che dà luogo al possibile uso, in particolare la gravità, la probabilità e l'entità del danno che sarebbe causato in caso di mancato uso del sistema;
 - b) le conseguenze dell'uso del sistema per i diritti e le libertà di tutte le persone interessate, in particolare la gravità, la probabilità e l'entità di tali conseguenze.

L'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto per uno qualsiasi degli obiettivi di cui al paragrafo 1, primo comma, lettera h), del presente articolo rispetta inoltre le tutele e le condizioni necessarie e proporzionate in relazione all'uso, conformemente al diritto nazionale che autorizza tale uso, in particolare per quanto riguarda le limitazioni temporali, geografiche e personali. L'uso del sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico è autorizzato solo se l'autorità di contrasto ha completato una valutazione d'impatto sui diritti fondamentali come previsto all'articolo 27 e ha registrato il sistema nella banca dati UE conformemente all'articolo 49. Tuttavia, in situazioni di urgenza debitamente giustificate, è possibile iniziare a usare tali sistemi senza la registrazione nella banca dati dell'UE, a condizione che tale registrazione sia completata senza indebito ritardo.

3. Ai fini del paragrafo 1, primo comma, lettera h), e del paragrafo 2, ogni uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità delle regole dettagliate del diritto nazionale di cui al paragrafo 5. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati.

L'autorità giudiziaria competente o un'autorità amministrativa indipendente la cui decisione è vincolante rilascia l'autorizzazione solo se ha accertato, sulla base di prove oggettive o indicazioni chiare che le sono state presentate, che l'uso del sistema di identificazione biometrica remota "in tempo reale" in questione è necessario e proporzionato al conseguimento di uno degli obiettivi di cui al paragrafo 1, primo comma, lettera h), come indicato nella richiesta e, in particolare, rimane limitato a quanto strettamente necessario per quanto riguarda il periodo di tempo e l'ambito geografico e personale. Nel decidere in merito alla richiesta, tale autorità tiene conto degli elementi di cui al paragrafo 2. Nessuna decisione che produca effetti giuridici negativi su una persona può essere presa unicamente sulla base dell'output del sistema di identificazione biometrica remota "in tempo reale".

4. Fatto salvo il paragrafo 3, ogni uso di un sistema di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto è notificato alla pertinente autorità di vigilanza del mercato e all'autorità nazionale per la protezione dei dati conformemente alle regole nazionali di cui al paragrafo 5. La notifica contiene almeno le informazioni di cui al paragrafo 6 e non include dati operativi sensibili.

5. Uno Stato membro può decidere di prevedere la possibilità di autorizzare in tutto o in parte l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, entro i limiti e alle condizioni di cui al paragrafo 1, primo comma, lettera h), e ai paragrafi 2 e 3. Gli Stati membri interessati stabiliscono nel proprio diritto nazionale le necessarie regole dettagliate per la richiesta, il rilascio, l'esercizio delle autorizzazioni di cui al paragrafo 3, nonché per le attività di controllo e comunicazione ad esse relative. Tali regole specificano inoltre per quali degli obiettivi elencati al paragrafo 1, primo comma, lettera h), compresi i reati di cui alla lettera h), punto iii), le autorità competenti possono essere autorizzate ad utilizzare tali sistemi a fini di attività di contrasto. Gli Stati membri notificano tali regole alla Commissione al più tardi 30 giorni dopo la loro adozione. Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota.
6. Le autorità nazionali di vigilanza del mercato e le autorità nazionali per la protezione dei dati degli Stati membri cui è stato notificato l'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto a norma del paragrafo 4, presentano alla Commissione relazioni annuali su tale uso. A tal fine, la Commissione fornisce agli Stati membri e alle autorità nazionali di vigilanza del mercato e di protezione dei dati un modello comprendente informazioni sul numero di decisioni che le autorità giudiziarie competenti, o un'autorità amministrativa indipendente la cui decisione è vincolante, hanno adottato in risposta alle richieste di autorizzazione a norma del paragrafo 3 e il loro esito.

7. La Commissione pubblica relazioni annuali sull'uso di sistemi di identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di contrasto, fondate sui dati aggregati negli Stati membri sulla base delle relazioni annuali di cui al paragrafo 6. Tali relazioni annuali non includono dati operativi sensibili delle relative attività di contrasto.
8. Il presente articolo lascia impregiudicati i divieti che si applicano qualora una pratica di IA violi altre disposizioni di diritto dell'Unione.

Capo III

Sistemi di IA ad alto rischio

SEZIONE 1

CLASSIFICAZIONE DEI SISTEMI DI IA COME "AD ALTO RISCHIO"

Articolo 6

Regole di classificazione per i sistemi di IA ad alto rischio

1. A prescindere dal fatto che sia immesso sul mercato o messo in servizio indipendentemente dai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:
 - a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

- b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I.
- 2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III.
- 3. In deroga al paragrafo 2, un sistema di IA di cui all'allegato III non è considerato ad alto rischio se non presenta un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale.

Il primo comma si applica quando è soddisfatta almeno una qualsiasi delle condizioni seguenti:

- a) il sistema di IA è destinato a eseguire un compito procedurale limitato;
- b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata;
- c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o
- d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III.

Fatto salvo il primo comma, un sistema di IA di cui all'allegato III è sempre considerato ad alto rischio qualora esso effettui profilazione di persone fisiche.

4. Un fornitore che ritiene che un sistema di IA di cui all'allegato III non sia ad alto rischio ne documenta la valutazione prima che tale sistema sia immesso sul mercato oppure messo in servizio. Tale fornitore è soggetto all'obbligo di registrazione di cui all'articolo 49, paragrafo 2. Su richiesta delle autorità nazionali competenti, il fornitore mette a disposizione la documentazione relativa alla valutazione.
5. Dopo aver consultato il consiglio europeo per l'intelligenza artificiale ("consiglio per l'IA"), ed entro ... [18 mesi dalla data di entrata in vigore del presente regolamento], la Commissione fornisce orientamenti che specificano l'attuazione pratica del presente articolo in linea con l'articolo 96, insieme a un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio.
6. Alla Commissione è conferito il potere di adottare atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo aggiungendo nuove condizioni a quelle ivi stabilite, oppure modificandole, qualora vi siano prove concrete e affidabili dell'esistenza di sistemi di IA che rientrano nell'ambito di applicazione dell'allegato III ma non presentano un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche.

7. La Commissione adotta atti delegati in conformità dell'articolo 97 al fine di modificare il paragrafo 3, secondo comma, del presente articolo sopprimendo qualsiasi condizione ivi stabilita, qualora vi siano prove concrete e affidabili che è necessario al fine di mantenere il livello di protezione della salute, della sicurezza e dei diritti fondamentali previsto dal presente regolamento.
8. Eventuali modifiche alle condizioni di cui al paragrafo 3, secondo comma, adottate in conformità dei paragrafi 6 e 7 del presente articolo non riducono il livello globale di protezione della salute, della sicurezza e dei diritti fondamentali nell'Unione previsto dal presente regolamento e garantiscono la coerenza con gli atti delegati adottati a norma dell'articolo 7, paragrafo 1, e tengono conto degli sviluppi tecnologici e del mercato.

Articolo 7

Modifiche dell'allegato III

1. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato III aggiungendo o modificando i casi d'uso dei sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:
 - a) i sistemi di IA sono destinati a essere usati in uno dei settori elencati nell'allegato III;
 - b) i sistemi di IA presentano un rischio di danno per la salute e la sicurezza, o di impatto negativo sui diritti fondamentali, e tale rischio è equivalente o superiore al rischio di danno o di impatto negativo presentato dai sistemi di IA ad alto rischio di cui all'allegato III.

2. Nel valutare la condizione di cui al paragrafo 1, lettera b), la Commissione tiene conto dei criteri seguenti:
- a) la finalità prevista del sistema di IA;
 - b) la misura in cui un sistema di IA è stato usato o è probabile che sarà usato;
 - c) la natura e la quantità di dati trattati e utilizzati dal sistema di IA, in particolare l'eventualità che siano trattate categorie particolari di dati personali;
 - d) la misura in cui il sistema di IA agisce autonomamente e la possibilità che un essere umano annulli una decisione o una raccomandazione che potrebbe causare un danno potenziale;
 - e) la misura in cui l'uso di un sistema di IA ha già causato un danno alla salute e alla sicurezza, ha avuto un impatto negativo sui diritti fondamentali o ha suscitato gravi preoccupazioni in relazione alla probabilità di tale danno o impatto negativo, come dimostrato, ad esempio, da relazioni o da prove documentate presentate alle autorità nazionali competenti o da altre relazioni, a seconda dei casi;
 - f) la portata potenziale di tale danno o di tale impatto negativo, in particolare in termini di intensità e capacità di incidere su più persone o di incidere in modo sproporzionato su un particolare gruppo di persone;
 - g) la misura in cui le persone che potrebbero subire il danno o l'impatto negativo dipendono dal risultato prodotto da un sistema di IA, in particolare in ragione del fatto che per motivi pratici o giuridici non è ragionevolmente possibile sottrarsi a tale risultato;

- h) la misura in cui esiste uno squilibrio di potere o le persone che potrebbero subire il danno o l'impatto negativo si trovano in una posizione vulnerabile rispetto al deployer di un sistema di IA, in particolare a causa della condizione, dell'autorità, della conoscenza, della situazione economica o sociale o dell'età;
- i) la misura in cui il risultato prodotto con il coinvolgimento di un sistema di IA è facilmente correggibile o reversibile, tenendo conto delle soluzioni tecniche disponibili per correggerlo o ribaltarlo, considerando non facilmente correggibili o reversibili i risultati che hanno un impatto negativo sulla salute, sulla sicurezza o sui diritti fondamentali;
- j) l'entità e la probabilità dei benefici derivanti dalla diffusione del sistema di IA per le persone, i gruppi o la società in generale, compresi i possibili miglioramenti della sicurezza del prodotto;
- k) la misura in cui il vigente diritto dell'Unione prevede:
 - i) misure di ricorso efficaci in relazione ai rischi presentati da un sistema di IA, ad esclusione delle richieste di risarcimento del danno;
 - ii) misure efficaci per prevenire o ridurre sostanzialmente tali rischi.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'elenco di cui all'allegato III rimuovendo sistemi di IA ad alto rischio se sono soddisfatte entrambe le condizioni seguenti:
- a) il sistema di IA ad alto rischio interessato non pone più rischi significativi per i diritti fondamentali, la salute o la sicurezza, tenendo conto dei criteri elencati al paragrafo 2;
 - b) la soppressione non riduce il livello generale di protezione della salute, della sicurezza e dei diritti fondamentali a norma del diritto dell'Unione.

SEZIONE 2

REQUISITI PER I SISTEMI DI IA AD ALTO RISCHIO

Articolo 8

Conformità ai requisiti

1. I sistemi di IA ad alto rischio rispettano i requisiti stabiliti nella presente sezione, tenendo conto delle loro previste finalità nonché dello stato dell'arte generalmente riconosciuto in materia di IA e di tecnologie correlate all'IA. Nel garantire conformità a tali requisiti si tiene conto del sistema di gestione dei rischi di cui all'articolo 9.

2. Se un prodotto contiene un sistema di IA cui si applicano i requisiti del presente regolamento e i requisiti della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, i fornitori sono responsabili di garantire che il loro prodotto sia pienamente conforme a tutti i requisiti applicabili previsti dalla normativa di armonizzazione dell'Unione applicabile. Nel garantire la conformità dei sistemi di IA ad alto rischio di cui al paragrafo 1 ai requisiti di cui alla presente sezione e al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari processi di prova e di comunicazione nonché le informazioni e la documentazione che forniscono relativamente al loro prodotto nella documentazione e nelle procedure esistenti e richieste in conformità della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A.

Articolo 9

Sistema di gestione dei rischi

1. In relazione ai sistemi di IA ad alto rischio è istituito, attuato, documentato e mantenuto un sistema di gestione dei rischi.
2. Il sistema di gestione dei rischi è inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. Esso comprende le fasi seguenti:
 - a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista;

- b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità prevista e in condizioni di uso improprio ragionevolmente prevedibile;
 - c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72;
 - d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lettera a).
3. I rischi di cui al presente articolo riguardano solo quelli che possono essere ragionevolmente attenuati o eliminati attraverso lo sviluppo o la progettazione del sistema di IA ad alto rischio o la fornitura di informazioni tecniche adeguate.
4. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), tengono in debita considerazione gli effetti e la possibile interazione derivanti dall'applicazione combinata dei requisiti di cui alla presente sezione, al fine di ridurre al minimo i rischi con maggiore efficacia e raggiungere nel contempo un equilibrio adeguato nell'attuazione delle misure volte a soddisfare tali requisiti.
5. Le misure di gestione dei rischi di cui al paragrafo 2, lettera d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili.

Nell'individuare le misure di gestione dei rischi più appropriate, occorre garantire quanto segue:

- a) l'eliminazione o la riduzione dei rischi individuati e valutati a norma del paragrafo 2, per quanto possibile dal punto di vista tecnico attraverso un'adeguata progettazione e fabbricazione del sistema di IA ad alto rischio;
- b) ove opportuno, l'attuazione di adeguate misure di attenuazione e di controllo nell'affrontare i rischi che non possono essere eliminati;
- c) la fornitura delle informazioni richieste a norma dell'articolo 13 e, ove opportuno, la formazione dei deployer.

Al fine di eliminare o ridurre i rischi connessi all'uso del sistema di IA ad alto rischio, si tengono debitamente in considerazione le conoscenze tecniche, l'esperienza, l'istruzione e la formazione che ci si può aspettare dal deployer e il contesto presumibile in cui il sistema è destinato ad essere usato.

- 6. I sistemi di IA ad alto rischio sono sottoposti a prova al fine di individuare le misure di gestione dei rischi più appropriate e mirate. Le prove garantiscono che i sistemi di IA ad alto rischio funzionino in modo coerente per la finalità prevista e che siano conformi ai requisiti di cui alla presente sezione.
- 7. Le procedure di prova possono comprendere prove in condizioni reali conformemente all'articolo 60.

8. Le prove dei sistemi di IA ad alto rischio sono effettuate, a seconda dei casi, in un qualsiasi momento dell'intero processo di sviluppo e, in ogni caso, prima della loro immissione sul mercato o messa in servizio. Le prove sono effettuate sulla base di metriche e soglie probabilistiche definite precedentemente e adeguate alla finalità prevista perseguita dal sistema di IA ad alto rischio.
9. Nell'attuare il sistema di gestione dei rischi di cui ai paragrafi da 1 a 7, i fornitori prestano attenzione, nell'ottica della sua finalità prevista, all'eventualità che il sistema di IA ad alto rischio possa avere un impatto negativo sulle persone di età inferiore a 18 anni o, a seconda dei casi, su altri gruppi vulnerabili.
10. Per i fornitori di sistemi di IA ad alto rischio soggetti ai requisiti relativi ai processi interni di gestione dei rischi a norma di altre disposizioni pertinenti del diritto dell'Unione, gli aspetti di cui ai paragrafi da 1 a 9 possono far parte delle procedure di gestione dei rischi stabilite a norma di tale diritto oppure essere combinati con le stesse.

Articolo 10

Dati e governance dei dati

1. I sistemi di IA ad alto rischio che utilizzano tecniche che prevedono l'uso di dati per l'addestramento di modelli di IA sono sviluppati sulla base di set di dati di addestramento, convalida e prova che soddisfano i criteri di qualità di cui ai paragrafi da 2 a 5 ogniqualvolta siano utilizzati tali set di dati.

2. I set di dati di addestramento, convalida e prova sono soggetti a pratiche di governance e gestione dei dati adeguate alla finalità prevista del sistema di IA ad alto rischio. Tali pratiche riguardano in particolare:
- a) le scelte progettuali pertinenti;
 - b) i processi di raccolta dei dati e l'origine dei dati, nonché la finalità originaria della raccolta nel caso di dati personali;
 - c) le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, aggiornamento, arricchimento e aggregazione;
 - d) la formulazione di ipotesi, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino;
 - e) una valutazione della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari;
 - f) un esame atto a valutare le possibili distorsioni suscettibili di incidere sulla salute e sulla sicurezza delle persone, di avere un impatto negativo sui diritti fondamentali o di comportare discriminazioni vietate dal diritto dell'Unione, specie laddove gli output di dati influenzano gli input per operazioni future;
 - g) le misure adeguate per individuare, prevenire e attenuare le possibili distorsioni individuate conformemente alla lettera f);
 - h) l'individuazione di lacune o carenze pertinenti nei dati tali da pregiudicare il rispetto del presente regolamento e il modo in cui tali lacune e carenze possono essere colmate.

3. I set di dati di addestramento, convalida e prova sono pertinenti, sufficientemente rappresentativi e, nella misura del possibile, esenti da errori e completi nell'ottica della finalità prevista. Essi possiedono le proprietà statistiche appropriate anche, ove applicabile, per quanto riguarda le persone o i gruppi di persone relativamente ai quali il sistema di IA ad alto rischio è destinato a essere usato. Queste caratteristiche dei set di dati possono essere soddisfatte a livello di singoli set di dati o a livello di una combinazione degli stessi.
4. I set di dati tengono conto, nella misura necessaria per la finalità prevista, delle caratteristiche o degli elementi particolari dello specifico ambito geografico, contestuale, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.
5. Nella misura in cui ciò sia strettamente necessario al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio in conformità del paragrafo 2, lettere f) e g), del presente articolo, i fornitori di tali sistemi possono eccezionalmente trattare categorie particolari di dati personali, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche. Oltre alle disposizioni di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680 devono essere soddisfatte, affinché tale trattamento avvenga, tutte le condizioni seguenti:
 - a) il rilevamento e la correzione delle distorsioni non possono essere realizzati efficacemente mediante il trattamento di altri dati, compresi i dati sintetici o anonimizzati;

- b) le categorie particolari di dati personali sono soggette a limitazioni tecniche relative al riutilizzo dei dati personali, nonché a misure più avanzate di sicurezza e di tutela della vita privata, compresa la pseudonimizzazione;
- c) le categorie particolari di dati personali sono soggette a misure tese a garantire che i dati personali trattati siano resi sicuri e protetti nonché soggetti a garanzie adeguate, ivi compresi controlli e documentazione rigorosi dell'accesso, al fine di evitare abusi e garantire che solo le persone autorizzate e sottostanti a opportuni obblighi di riservatezza abbiano accesso a tali dati personali;
- d) le categorie particolari di dati personali non devono essere trasmesse, trasferite o altrimenti consultate da terzi;
- e) le categorie particolari di dati personali vengono cancellate dopo che la distorsione è stata corretta oppure i dati personali hanno raggiunto la fine del loro periodo di conservazione, a seconda di quale delle due condizioni si verifica per prima;
- f) i registri delle attività di trattamento a norma dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680 comprendono i motivi per cui il trattamento delle categorie particolari di dati personali era strettamente necessario per rilevare e correggere distorsioni e i motivi per cui tale obiettivo non poteva essere raggiunto mediante il trattamento di altri dati.

6. Per lo sviluppo di sistemi di IA ad alto rischio che non utilizzano tecniche che prevedono l'addestramento di modelli di IA, i paragrafi da 2 a 5 si applicano solo ai set di dati di prova.

Articolo 11
Documentazione tecnica

1. La documentazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio di tale sistema ed è tenuta aggiornata.

La documentazione tecnica è redatta in modo da dimostrare che il sistema di IA ad alto rischio è conforme ai requisiti di cui alla presente sezione e da fornire alle autorità nazionali competenti e agli organismi notificati, in forma chiara e comprensibile, le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. Essa contiene almeno gli elementi di cui all'allegato IV. Le PMI, comprese le start-up, possono fornire in modo semplificato gli elementi della documentazione tecnica specificati nell'allegato IV. A tal fine la Commissione definisce un modulo di documentazione tecnica semplificata che risponda alle esigenze delle piccole imprese e delle microimprese. Qualora una PMI, compresa una start-up, decida di fornire in modo semplificato le informazioni richieste nell'allegato IV, utilizza il modulo di cui al presente paragrafo. Gli organismi notificati accettano il modulo ai fini della valutazione della conformità.

2. Se è immesso sul mercato o messo in servizio un sistema di IA ad alto rischio connesso a un prodotto contemplato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, si redige un'unica documentazione tecnica contenente tutte le informazioni di cui al paragrafo 1 e le informazioni necessarie a norma di tali atti giuridici.

3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato IV ove necessario per garantire che, alla luce del progresso tecnico, la documentazione tecnica fornisca tutte le informazioni necessarie per valutare la conformità del sistema ai requisiti di cui alla presente sezione.

Articolo 12

Conservazione delle registrazioni

1. I sistemi di IA ad alto rischio consentono a livello tecnico la registrazione automatica degli eventi ("log") per la durata del ciclo di vita del sistema.
2. Al fine di garantire un livello di tracciabilità del funzionamento del sistema di IA ad alto rischio adeguato alla finalità prevista del sistema, le capacità di registrazione consentono la registrazione di eventi pertinenti per:
 - a) l'individuazione di situazioni che possono far sì che il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, o determinare una modifica sostanziale;
 - b) l'agevolazione del monitoraggio successivo all'immissione sul mercato di cui all'articolo 72; e
 - c) il monitoraggio del funzionamento dei sistemi di IA ad alto rischio di cui all'articolo 26, paragrafo 5.
3. Per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le capacità di registrazione comprendono almeno i dati seguenti:
 - a) la registrazione del periodo di ciascun utilizzo del sistema (data e ora di inizio e di fine di ciascun utilizzo);

- b) la banca dati di riferimento utilizzata dal sistema per verificare i dati di input;
- c) i dati di input per i quali la ricerca ha portato a una corrispondenza;
- d) l'identificativo delle persone fisiche che partecipano alla verifica dei risultati di cui all'articolo 14, paragrafo 5.

Articolo 13

Trasparenza e fornitura di informazioni ai deployer

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire ai deployer di interpretare l'output del sistema e utilizzarlo adeguatamente. Sono garantiti un tipo e un livello di trasparenza adeguati, che consentano di conseguire il rispetto dei pertinenti obblighi del fornitore e del deployer di cui alla sezione 3.
2. I sistemi di IA ad alto rischio sono accompagnati da istruzioni per l'uso, in un formato appropriato digitale o non digitale, che comprendono informazioni concise, complete, corrette e chiare che siano pertinenti, accessibili e comprensibili per i deployer.
3. Le istruzioni per l'uso contengono almeno le informazioni seguenti:
 - a) l'identità e i dati di contatto del fornitore e, ove applicabile, del suo rappresentante autorizzato;

- b) le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui:
- i) la finalità prevista;
 - ii) il livello di accuratezza che ci si può attendere, comprese le metriche, di robustezza e cibersecurity di cui all'articolo 15 rispetto al quale il sistema di IA ad alto rischio è stato sottoposto a prova e convalidato, e qualsiasi circostanza nota e prevedibile che possa avere un impatto sul livello atteso di accuratezza, robustezza e cibersecurity;
 - iii) qualsiasi circostanza nota o prevedibile connessa all'uso del sistema di IA ad alto rischio in conformità della sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile che possa comportare rischi per la salute e la sicurezza o per i diritti fondamentali di cui all'articolo 9, paragrafo 2;
 - iv) se del caso, le capacità e caratteristiche tecniche del sistema di IA ad alto rischio connesse alla fornitura di informazioni pertinenti per spiegarne l'output;
 - v) ove opportuno, le sue prestazioni per quanto riguarda le persone o i gruppi di persone specifici sui quali il sistema è destinato a essere utilizzato;
 - vi) ove opportuno, le specifiche per i dati di input o qualsiasi altra informazione pertinente in termini di set di dati di addestramento, convalida e prova, tenendo conto della finalità prevista del sistema di IA ad alto rischio;

- vii) se del caso, informazioni che consentano ai deployer di interpretare l'output del sistema di IA ad alto rischio e di usarlo in modo opportuno;
- c) le eventuali modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni, che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità;
- d) le misure di sorveglianza umana di cui all'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA ad alto rischio da parte dei deployer;
- e) le risorse computazionali e di hardware necessarie, la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e cura, compresa la relativa frequenza, necessarie per garantire il corretto funzionamento di tale sistema, anche per quanto riguarda gli aggiornamenti software;
- f) se del caso, una descrizione dei meccanismi inclusi nel sistema di IA ad alto rischio che consente ai deployer di raccogliere, conservare e interpretare correttamente i log in conformità dell'articolo 12.

Articolo 14

Sorveglianza umana

1. I sistemi di IA ad alto rischio sono progettati e sviluppati, anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.

2. La sorveglianza umana mira a prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile, in particolare qualora tali rischi persistano nonostante l'applicazione di altri requisiti di cui alla presente sezione.
3. Le misure di sorveglianza sono commisurate ai rischi, al livello di autonomia e al contesto di utilizzo del sistema di IA ad alto rischio e sono garantite mediante almeno uno dei tipi di misure seguenti:
 - a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile;
 - b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal deployer.
4. Ai fini dell'attuazione dei paragrafi 1, 2 e 3, il sistema di IA ad alto rischio è fornito al deployer in modo tale che le persone fisiche alle quali è affidata la sorveglianza umana abbiano la possibilità, ove opportuno e proporzionato, di:
 - a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese;

- b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ("distorsione dell'automazione"), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche;
- c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili;
- d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio;
- e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di "arresto" o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza.

5. In aggiunta, per i sistemi di IA ad alto rischio di cui all'allegato III, punto 1, lettera a), le misure di cui al paragrafo 3 del presente articolo sono tali da garantire che il deployer non compia azioni o adotti decisioni sulla base dell'identificazione risultante dal sistema, a meno che tale identificazione non sia stata verificata e confermata separatamente da almeno due persone fisiche dotate della necessaria competenza, formazione e autorità.

Il requisito di una verifica separata da parte di almeno due persone fisiche non si applica ai sistemi di IA ad alto rischio utilizzati a fini di contrasto, migrazione, controllo delle frontiere o asilo, qualora il diritto dell'Unione o nazionale ritenga sproporzionata l'applicazione di tale requisito.

Articolo 15

Accuratezza, robustezza e cibersecurity

1. I sistemi di IA ad alto rischio sono progettati e sviluppati in modo tale da conseguire un adeguato livello di accuratezza, robustezza e cibersecurity e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita.
2. Al fine di affrontare gli aspetti tecnici relativi alle modalità di misurazione degli adeguati livelli di accuratezza e robustezza di cui al paragrafo 1 e altre metriche di prestazione pertinenti, la Commissione, in cooperazione con i portatori di interessi e le organizzazioni pertinenti, quali le autorità di metrologia e di analisi comparativa, incoraggia, se del caso, lo sviluppo di parametri di riferimento e metodologie di misurazione.
3. I livelli di accuratezza e le pertinenti metriche di accuratezza dei sistemi di IA ad alto rischio sono dichiarati nelle istruzioni per l'uso che accompagnano il sistema.
4. I sistemi di IA ad alto rischio sono il più resilienti possibile per quanto riguarda errori, guasti o incongruenze che possono verificarsi all'interno del sistema o nell'ambiente in cui esso opera, in particolare a causa della loro interazione con persone fisiche o altri sistemi. A tale riguardo sono adottate misure tecniche e organizzative.

La robustezza dei sistemi di IA ad alto rischio può essere conseguita mediante soluzioni tecniche di ridondanza, che possono includere piani di backup o fail-safe.

I sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio sono sviluppati in modo tale da eliminare o ridurre il più possibile il rischio di output potenzialmente distorti che influenzano gli input per operazioni future (feedback loops - "circuiti di feedback") e garantire che tali circuiti di feedback siano oggetto di adeguate misure di attenuazione.

5. I sistemi di IA ad alto rischio sono resilienti ai tentativi di terzi non autorizzati di modificarne l'uso, gli output o le prestazioni sfruttando le vulnerabilità del sistema.

Le soluzioni tecniche volte a garantire la cibersecurity dei sistemi di IA ad alto rischio sono adeguate alle circostanze e ai rischi pertinenti.

Le soluzioni tecniche finalizzate ad affrontare le vulnerabilità specifiche dell'IA includono, ove opportuno, misure volte a prevenire, accertare, rispondere, risolvere e controllare gli attacchi che cercano di manipolare il set di dati di addestramento (data poisoning - "avvelenamento dei dati") o i componenti preaddestrati utilizzati nell'addestramento (model poisoning - "avvelenamento dei modelli"), gli input progettati in modo da far sì che il modello di IA commetta un errore (adversarial examples - "esempi antagonisti", o model evasion, - "evasione dal modello"), gli attacchi alla riservatezza o i difetti del modello.

SEZIONE 3

OBBLIGHI DEI FORNITORI E DEI DEPLOYER DEI SISTEMI DI IA AD ALTO RISCHIO E DI ALTRE PARTI

Articolo 16

Obblighi dei fornitori dei sistemi di IA ad alto rischio

I fornitori dei sistemi di IA ad alto rischio:

- a) garantiscono che i loro sistemi di IA ad alto rischio siano conformi ai requisiti di cui alla sezione 2;
- b) indicano sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento, a seconda dei casi, il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati;
- c) dispongono di un sistema di gestione della qualità conforme all'articolo 17;
- d) conservano la documentazione di cui all'articolo 18;
- e) quando sono sotto il loro controllo, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio di cui all'articolo 19;
- f) garantiscono che il sistema di IA ad alto rischio sia sottoposto alla pertinente procedura di valutazione della conformità di cui all'articolo 43 prima che sia immesso sul mercato o messo in servizio;

- g) elaborano una dichiarazione di conformità UE a norma dell'articolo 47;
- h) appongono la marcatura CE sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento per indicare la conformità al presente regolamento a norma dell'articolo 48;
- i) rispettano gli obblighi di registrazione di cui all'articolo 49, paragrafo 1;
- j) adottano le necessarie misure correttive e forniscono le informazioni necessarie in conformità dell'articolo 20;
- k) su richiesta motivata di un'autorità nazionale competente, dimostrano la conformità del sistema di IA ad alto rischio ai requisiti di cui alla sezione 2;
- l) garantiscono che il sistema di IA ad alto rischio sia conforme ai requisiti di accessibilità in conformità delle direttive (UE) 2016/2102 e (UE) 2019/882.

Articolo 17

Sistema di gestione della qualità

1. I fornitori di sistemi di IA ad alto rischio istituiscono un sistema di gestione della qualità che garantisce la conformità al presente regolamento. Tale sistema è documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende almeno gli aspetti seguenti:
 - a) una strategia per la conformità normativa, compresa la conformità alle procedure di valutazione della conformità e alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio;

- b) le tecniche, le procedure e gli interventi sistematici da utilizzare per la progettazione, il controllo della progettazione e la verifica della progettazione del sistema di IA ad alto rischio;
- c) le tecniche, le procedure e gli interventi sistematici da utilizzare per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio;
- d) le procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA ad alto rischio e la frequenza con cui devono essere effettuate;
- e) le specifiche tecniche, comprese le norme, da applicare e, qualora le pertinenti norme armonizzate non siano applicate integralmente, o non includano tutti i requisiti pertinenti di cui alla sezione 2, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme a tali requisiti;
- f) i sistemi e le procedure per la gestione dei dati, compresa l'acquisizione, la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio;
- g) il sistema di gestione dei rischi di cui all'articolo 9;
- h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato a norma dell'articolo 72;

- i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 73;
 - j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, comprese quelle che forniscono o sostengono l'accesso ai dati, gli organismi notificati, altri operatori, clienti o altre parti interessate;
 - k) i sistemi e le procedure per la conservazione delle registrazioni e di tutte le informazioni e la documentazione pertinenti;
 - l) la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento;
 - m) un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale per quanto riguarda tutti gli aspetti elencati nel presente paragrafo.
2. L'attuazione degli aspetti di cui al paragrafo 1 è proporzionata alle dimensioni dell'organizzazione del fornitore. I fornitori rispettano, in ogni caso, il grado di rigore e il livello di protezione necessari per garantire la conformità dei loro sistemi di IA ad alto rischio al presente regolamento.
3. I fornitori di sistemi di IA ad alto rischio soggetti agli obblighi relativi ai sistemi di gestione della qualità o a una funzione equivalente a norma del pertinente diritto settoriale dell'Unione possono includere gli aspetti elencati al paragrafo 1 nell'ambito dei sistemi di gestione della qualità stabiliti a norma di tale diritto.

4. Per i fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di istituire un sistema di gestione della qualità, ad eccezione del paragrafo 1, lettere g), h) e i), del presente articolo, si considera soddisfatto se sono soddisfatte le regole sui dispositivi o i processi di governance interna a norma del pertinente diritto dell'Unione in materia di servizi finanziari. A tal fine, si tiene conto delle norme armonizzate di cui all'articolo 40.

Articolo 18

Conservazione dei documenti

1. Il fornitore, per un periodo che termina 10 anni dopo che il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio, tiene a disposizione delle autorità nazionali competenti:
- a) la documentazione tecnica di cui all'articolo 11;
 - b) la documentazione relativa al sistema di gestione della qualità di cui all'articolo 17;
 - c) la documentazione relativa alle modifiche approvate dagli organismi notificati, ove applicabile;
 - d) le decisioni e gli altri documenti rilasciati dagli organismi notificati, ove applicabile;
 - e) la dichiarazione di conformità UE di cui all'articolo 47.

2. Ciascuno Stato membro stabilisce le condizioni alle quali la documentazione di cui al paragrafo 1 resta a disposizione delle autorità nazionali competenti per il periodo indicato in tale paragrafo nel caso in cui il prestatore o il rappresentante autorizzato stabilito nel suo territorio fallisca o cessi la sua attività prima della fine di tale periodo.
3. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, conservano la documentazione tecnica nell'ambito della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari.

Articolo 19

Log generati automaticamente

1. I fornitori di sistemi di IA ad alto rischio conservano i log di cui all'articolo 12, paragrafo 1, generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo. Fatto salvo il diritto dell'Unione o nazionale applicabile, i log sono conservati per un periodo adeguato alla finalità prevista del sistema di IA ad alto rischio, della durata di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.
2. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, a dispositivi o a processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio nell'ambito della documentazione conservata a norma del pertinente diritto in materia di servizi finanziari.

Articolo 20

Misure correttive e dovere di informazione

1. I fornitori di sistemi di IA ad alto rischio che ritengono o hanno motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio non sia conforme al presente regolamento adottano immediatamente le misure correttive necessarie per rendere conforme tale dispositivo, ritirarlo, disabilitarlo o richiamarlo, a seconda dei casi. Essi informano di conseguenza i distributori del sistema di IA ad alto rischio interessato e, ove applicabile, i deployer, il rappresentante autorizzato e gli importatori.
2. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, e il fornitore ne venga a conoscenza, tale fornitore indaga immediatamente sulle cause, in collaborazione con il deployer che ha effettuato la segnalazione, se del caso, e ne informa le autorità di vigilanza del mercato competenti per il sistema di IA ad alto rischio interessato e, ove applicabile, l'organismo notificato che ha rilasciato un certificato per il sistema di IA ad alto rischio in conformità dell'articolo 44, in particolare in merito alla natura della non conformità e all'eventuale misura correttiva pertinente adottata.

Articolo 21

Cooperazione con le autorità competenti

1. I fornitori di sistemi di IA ad alto rischio, su richiesta motivata di un'autorità competente, forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, in una lingua che può essere compresa facilmente dall'autorità in una delle lingue ufficiali delle istituzioni dell'Unione indicata dallo Stato membro interessato.
2. Su richiesta motivata di un'autorità competente, i fornitori concedono inoltre all'autorità competente richiedente, a seconda dei casi, l'accesso ai log generati automaticamente del sistema di IA ad alto rischio di cui all'articolo 12, paragrafo 1, nella misura in cui tali log sono sotto il loro controllo.
3. Qualsiasi informazione ottenuta da un'autorità competente a norma del presente articolo è trattata in conformità degli obblighi di riservatezza di cui all'articolo 78.

Articolo 22

Rappresentanti autorizzati dei fornitori dei sistemi di IA ad alto rischio

1. Prima di mettere a disposizione i sistemi di IA ad alto rischio sul mercato dell'Unione, i fornitori stabiliti in paesi terzi nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

2. Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore.
3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fornitore. Fornisce una copia del mandato alle autorità di vigilanza del mercato, su richiesta, in una delle lingue ufficiali delle istituzioni dell'Unione indicata dall'autorità competente. Ai fini del presente regolamento, il mandato consente al rappresentante autorizzato di eseguire i compiti seguenti:
 - a) verificare che la dichiarazione di conformità UE di cui all'articolo 47 e la documentazione tecnica di cui all'articolo 11 siano state redatte e che il fornitore abbia eseguito un'appropriata procedura di valutazione della conformità;
 - b) tenere a disposizione delle autorità competenti e delle autorità o degli organismi nazionali di cui all'articolo 74, paragrafo 10, per un periodo di 10 anni dopo la data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, i dati di contatto del fornitore che ha nominato il rappresentante autorizzato, una copia della dichiarazione di conformità UE di cui all'articolo 47, la documentazione tecnica e, se del caso, il certificato rilasciato dall'organismo notificato;
 - c) fornire all'autorità competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui alla lettera b) del presente comma, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, compreso l'accesso ai log, di cui all'articolo 12, paragrafo 1, generati automaticamente dal sistema di IA ad alto rischio nella misura in cui tali log sono sotto il controllo del fornitore;

- d) cooperare con le autorità competenti, su richiesta motivata, in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio, in particolare per ridurre e attenuare i rischi posti dal sistema di IA ad alto rischio;
- e) ove applicabile, rispettare gli obblighi di registrazione di cui all'articolo 49, paragrafo 1, o, se la registrazione è effettuata dal fornitore stesso, garantire la correttezza delle informazioni di cui all'allegato VIII, sezione A, punto 3.

Il mandato consente al rappresentante autorizzato di fare da interlocutore, in aggiunta o in sostituzione del fornitore, con le autorità competenti per tutte le questioni relative al rispetto del presente regolamento.

- 4. Il rappresentante autorizzato pone fine al mandato se ritiene o ha motivi per ritenere che il fornitore agisca in contrasto con i propri obblighi a norma del presente regolamento. In tal caso, comunica immediatamente alla pertinente autorità di vigilanza del mercato, nonché, se del caso, all'organismo notificato pertinente, la cessazione del mandato e i relativi motivi.

Articolo 23

Obblighi degli importatori

- 1. Prima di immettere sul mercato un sistema di IA ad alto rischio, gli importatori garantiscono che il sistema sia conforme al presente regolamento verificando che:
 - a) il fornitore di tale sistema di IA ad alto rischio abbia eseguito la pertinente procedura di valutazione della conformità di cui all'articolo 43;

- b) il fornitore abbia redatto la documentazione tecnica conformemente all'articolo 11 e all'allegato IV;
 - c) il sistema rechi la necessaria marcatura CE e sia accompagnato dalla dichiarazione di conformità UE di cui all'articolo 47 e dalle istruzioni per l'uso;
 - d) il fornitore abbia nominato un rappresentante autorizzato conformemente all'articolo 22, paragrafo 1.
2. Qualora abbia motivo sufficiente di ritenere che un sistema di IA ad alto rischio non sia conforme al presente regolamento, ovvero sia falsificato o sia accompagnato da una documentazione falsificata, un importatore non lo immette sul mercato fino a quando non sia stato reso conforme. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, l'importatore ne informa il fornitore del sistema, i rappresentanti autorizzati e le autorità di vigilanza del mercato.
3. Gli importatori indicano il loro nome, la loro denominazione commerciale registrata o il loro marchio registrato e l'indirizzo al quale possono essere contattati, sul sistema di IA ad alto rischio e sul suo imballaggio o in un documento di accompagnamento, ove applicabile.
4. Gli importatori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità ai requisiti di cui alla sezione 2.

5. Gli importatori conservano, per un periodo di 10 anni dalla data di immissione sul mercato o di messa in servizio del sistema di IA ad alto rischio, una copia del certificato rilasciato dall'organismo notificato, se del caso, delle istruzioni per l'uso e della dichiarazione di conformità UE di cui all'articolo 47.
6. Gli importatori forniscono alla pertinente autorità competente, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui al paragrafo 5, necessarie per dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2 in una lingua che può essere compresa facilmente da tale autorità nazionale competente. A tal fine garantiscono altresì che la documentazione tecnica possa essere messa a disposizione di tale autorità.
7. Gli importatori cooperano con le pertinenti autorità competenti in qualsiasi azione intrapresa da tali autorità in relazione a un sistema di IA ad alto rischio immesso sul mercato dagli importatori, in particolare per ridurre e attenuare i rischi che esso comporta.

Articolo 24

Obblighi dei distributori

1. Prima di mettere a disposizione sul mercato un sistema di IA ad alto rischio, i distributori verificano che esso rechi la necessaria marcatura CE, che sia accompagnato da una copia della dichiarazione di conformità UE di cui all'articolo 47 e dalle istruzioni per l'uso e che il fornitore e l'importatore di tale sistema, a seconda dei casi, abbiano rispettato i loro rispettivi obblighi di cui all'articolo 16, lettere b) e c), e all'articolo 23, paragrafo 3.

2. Qualora ritenga o abbia motivo di ritenere, sulla base delle informazioni in suo possesso, che un sistema di IA ad alto rischio non sia conforme ai requisiti di cui alla sezione 2, un distributore non lo mette a disposizione sul mercato fino a quando tale sistema di IA ad alto rischio non sia stato reso conforme a tali requisiti. Inoltre, qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, il distributore ne informa il fornitore o l'importatore del sistema, a seconda dei casi.
3. I distributori garantiscono che, fintantoché un sistema di IA ad alto rischio è sotto la loro responsabilità, le condizioni di stoccaggio o di trasporto, ove applicabili, non pregiudichino la conformità del sistema ai requisiti di cui alla sezione 2.
4. Un distributore che ritiene o ha motivo di ritenere, sulla base delle informazioni in suo possesso, che un sistema di IA ad alto rischio che ha messo a disposizione sul mercato non sia conforme ai requisiti di cui alla sezione 2, adotta le misure correttive necessarie per rendere tale sistema conforme a tali requisiti, ritirarlo o richiamarlo o garantisce che il fornitore, l'importatore o qualsiasi operatore pertinente, a seconda dei casi, adotti tali misure correttive. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, il distributore ne informa immediatamente il fornitore o l'importatore del sistema e le autorità competenti per il sistema di IA ad alto rischio interessate fornendo in particolare informazioni precise sulla non conformità e sulle eventuali misure correttive adottate.

5. Su richiesta motivata di una pertinente autorità competente, i distributori di un sistema di IA ad alto rischio forniscono a tale autorità tutte le informazioni e la documentazione concernenti le sue azioni a norma dei paragrafi da 1 a 4 necessarie per dimostrare la conformità di tale sistema ai requisiti di cui alla sezione 2.
6. I distributori cooperano con le pertinenti autorità competenti in qualsiasi azione intrapresa da tali autorità in relazione a un sistema di IA ad alto rischio messo a disposizione sul mercato dai distributori, in particolare per ridurre e attenuare il rischio che esso comporta.

Articolo 25

Responsabilità lungo la catena del valore dell'IA

1. Qualsiasi distributore, importatore, deployer o altro terzo è considerato fornitore di un sistema di IA ad alto rischio ai fini del presente regolamento ed è soggetto agli obblighi del fornitore a norma dell'articolo 16, nelle circostanze seguenti:
 - a) se appone il proprio nome o marchio su un sistema di IA ad alto rischio già immesso sul mercato o messo in servizio, fatti salvi accordi contrattuali che prevedano una diversa ripartizione degli obblighi al riguardo;
 - b) se apporta una modifica sostanziale a un sistema di IA ad alto rischio già immesso sul mercato o già messo in servizio in modo tale che resti un sistema di IA ad alto rischio a norma dell'articolo 6;

- c) se modifica la finalità prevista di un sistema di IA, anche un sistema per finalità generali, che non è stato classificato come ad alto rischio e che è già stato immesso sul mercato o messo in servizio in modo tale che il sistema di IA interessato diventi un sistema di IA ad alto rischio a norma dell'articolo 6.
2. Qualora si verificano le circostanze di cui al paragrafo 1, il fornitore che ha inizialmente immesso sul mercato o messo in servizio il sistema di IA non è più considerato fornitore di quel determinato sistema di IA ai fini del presente regolamento. Tale fornitore iniziale coopera strettamente con i nuovi fornitori e mette a disposizione le informazioni necessarie nonché fornisce l'accesso tecnico ragionevolmente atteso e qualsiasi altra forma di assistenza che sono richiesti per l'adempimento degli obblighi di cui al presente regolamento, in particolare per quanto riguarda la conformità alla valutazione della conformità dei sistemi di IA ad alto rischio. Il presente paragrafo non si applica nei casi in cui il fornitore iniziale abbia chiaramente specificato che il suo sistema di IA non deve essere trasformato in un sistema di IA ad alto rischio e pertanto non sia soggetto all'obbligo di consegnare la documentazione.
3. Nel caso dei sistemi di IA ad alto rischio che sono componenti di sicurezza di prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fabbricante del prodotto è considerato il fornitore del sistema di IA ad alto rischio ed è soggetto agli obblighi di cui all'articolo 16, in una delle circostanze seguenti:
- a) se il sistema di IA ad alto rischio è immesso sul mercato insieme al prodotto con il nome o il marchio del fabbricante del prodotto;
 - b) se il sistema di IA ad alto rischio è messo in servizio con il nome o il marchio del fabbricante del prodotto dopo che il prodotto è stato immesso sul mercato.

4. Il fornitore di un sistema di IA ad alto rischio e il terzo che fornisce un sistema di IA, strumenti, servizi, componenti o processi utilizzati o integrati in un sistema di IA ad alto rischio precisano, mediante accordo scritto, le informazioni, le capacità, l'accesso tecnico e qualsiasi altra forma di assistenza necessari, sulla base dello stato dell'arte generalmente riconosciuto per permettere al fornitore del sistema di IA ad alto rischio di adempiere pienamente agli obblighi di cui al presente regolamento. Il presente paragrafo non si applica ai terzi che rendono accessibili al pubblico strumenti, servizi, processi o componenti, diversi dai modelli di IA per finalità generali, con licenza libera e open source.

L'ufficio per l'IA può elaborare e raccomandare clausole contrattuali tipo volontarie tra i fornitori di sistemi di IA ad alto rischio e i terzi che forniscono strumenti, servizi, componenti o processi utilizzati o integrati in sistemi di IA ad alto rischio. Nell'elaborare tali clausole contrattuali tipo volontarie, l'ufficio per l'IA tiene conto dei possibili requisiti contrattuali applicabili in determinati settori o casi commerciali. Le clausole contrattuali tipo volontarie sono pubblicati e disponibili gratuitamente in un formato elettronico facilmente utilizzabile.

5. I paragrafi 2 e 3 lasciano impregiudicata la necessità di rispettare e proteggere i diritti di proprietà intellettuale, le informazioni commerciali riservate e i segreti commerciali conformemente al diritto dell'Unione e nazionale.

Articolo 26

Obblighi dei deployer dei sistemi di IA ad alto rischio

1. I deployer di sistemi di IA ad alto rischio adottano idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi, a norma dei paragrafi 3 e 6.

2. I deployer affidano la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario.
3. Gli obblighi di cui ai paragrafi 1 e 2 lasciano impregiudicati gli altri obblighi dei deployer previsti dal diritto dell'Unione o nazionale e la libertà del deployer di organizzare le proprie risorse e attività al fine di attuare le misure di sorveglianza umana indicate dal fornitore.
4. Fatti salvi i paragrafi 1 e 2, nella misura in cui esercita il controllo sui dati di input, il deployer garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista del sistema di IA ad alto rischio.
5. I deployer monitorano il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informano i fornitori a tale riguardo conformemente all'articolo 72. Qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa comportare che il sistema di IA presenti un rischio ai sensi dell'articolo 79, paragrafo 1, i deployer ne informano, senza indebito ritardo, il fornitore o il distributore e la pertinente autorità di vigilanza del mercato e sospendono l'uso di tale sistema. Qualora abbiano individuato un incidente grave, i deployer ne informano immediatamente anche il fornitore, in primo luogo, e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato. Nel caso in cui il deployer non sia in grado di raggiungere il fornitore, si applica mutatis mutandis l'articolo 73. Tale obbligo non riguarda i dati operativi sensibili dei deployer dei sistemi di IA che sono autorità di contrasto.

Per i deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di monitoraggio di cui al primo comma si considera soddisfatto se sono soddisfatte le regole sui dispositivi, sui processi e sui meccanismi di governance interna a norma del pertinente diritto in materia di servizi finanziari.

6. I deployer di sistemi di IA ad alto rischio conservano i log generati automaticamente da tale sistema di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo, per un periodo adeguato alla prevista finalità del sistema di IA ad alto rischio, di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali.

I deployer che sono istituti finanziari soggetti a requisiti in materia di governance, di dispositivi o di processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari conservano i log come parte della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari.

7. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro, i deployer che sono datori di lavoro informano i rappresentanti dei lavoratori e i lavoratori interessati che saranno soggetti all'uso del sistema di IA ad alto rischio. Tali informazioni sono fornite, se del caso, conformemente alle norme e alle procedure stabilite dal diritto e dalle prassi dell'Unione e nazionali in materia di informazione dei lavoratori e dei loro rappresentanti.

8. I deployer di sistemi di IA ad alto rischio che sono autorità pubbliche o istituzioni, organi e organismi dell'Unione rispettano gli obblighi di registrazione di cui all'articolo 49. Ove accertino che il sistema di IA ad alto rischio che intendono utilizzare non è stato registrato nella banca dati dell'UE di cui all'articolo 71, tali deployer non utilizzano tale sistema e ne informano il fornitore o il distributore.
9. Se del caso, i deployer di sistemi di IA ad alto rischio usano le informazioni fornite a norma dell'articolo 13 del presente regolamento per adempiere al loro obbligo di effettuare una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680.
10. Fatta salva la direttiva (UE) 2016/680, nel quadro di un'indagine per la ricerca mirata di una persona sospettata o condannata per aver commesso un reato, il deployer di un sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori chiede un'autorizzazione, *ex ante* o senza indebito ritardo ed entro 48 ore, da parte di un'autorità giudiziaria o amministrativa la cui decisione è vincolante e soggetta a controllo giurisdizionale, per l'uso di tale sistema, tranne quando è utilizzato per l'identificazione iniziale di un potenziale sospetto sulla base di fatti oggettivi e verificabili direttamente connessi al reato. Ogni uso è limitato a quanto strettamente necessario per le indagini su uno specifico reato.

Se l'autorizzazione richiesta a norma del primo comma è respinta, l'uso del sistema di identificazione biometrica remota a posteriori collegato a tale autorizzazione richiesta è interrotto con effetto immediato e i dati personali connessi all'uso del sistema di IA ad alto rischio per il quale è stata richiesta l'autorizzazione sono cancellati.

In nessun caso tale sistema di IA ad alto rischio per l'identificazione biometrica remota a posteriori è utilizzato a fini di contrasto in modo non mirato, senza alcun collegamento con un reato, un procedimento penale, una minaccia reale e attuale o reale e prevedibile di un reato o la ricerca di una determinata persona scomparsa. Occorre garantire che nessuna decisione che produca effetti giuridici negativi su una persona possa essere presa dalle autorità di contrasto unicamente sulla base dell'output di tali sistemi di identificazione biometrica remota a posteriori.

Il presente paragrafo lascia impregiudicati l'articolo 9 del regolamento (UE) 2016/679 e l'articolo 10 della direttiva (UE) 2016/680 riguardo al trattamento dei dati biometrici.

Indipendentemente dalla finalità o dal deployer, ciascun uso di tali sistemi di IA ad alto rischio è documentato nel pertinente fascicolo di polizia e messo a disposizione della pertinente autorità di vigilanza del mercato e dell'autorità nazionale per la protezione dei dati, su richiesta, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Il presente comma lascia impregiudicati i poteri conferiti alle autorità di controllo dalla direttiva (UE) 2016/680.

I deployer presentano alle pertinenti autorità di vigilanza del mercato e alle autorità nazionali per la protezione dei dati relazioni annuali sul loro uso di sistemi di identificazione biometrica remota a posteriori, escludendo la divulgazione di dati operativi sensibili relativi alle attività di contrasto. Le relazioni possono essere aggregate per coprire più di un utilizzo.

Gli Stati membri possono introdurre, in conformità del diritto dell'Unione, disposizioni più restrittive sull'uso dei sistemi di identificazione biometrica remota a posteriori.

11. Fatto salvo l'articolo 50, del presente regolamento i deployer dei sistemi di IA ad alto rischio di cui all'allegato III che adottano decisioni o assistono nell'adozione di decisioni che riguardano persone fisiche informano queste ultime che sono soggette all'uso del sistema di IA ad alto rischio. Per i sistemi di IA ad alto rischio utilizzati a fini di contrasto si applica l'articolo 13 della direttiva (UE) 2016/680.
12. I deployer cooperano con le pertinenti autorità competenti in merito a qualsiasi azione intrapresa da dette autorità in relazione al sistema di IA ad alto rischio ai fini dell'attuazione del presente regolamento.

Articolo 27

Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio

1. Prima di utilizzare un sistema di IA ad alto rischio di cui all'articolo 6, paragrafo 2, ad eccezione dei sistemi di IA ad alto rischio destinati a essere usati nel settore elencati nell'allegato III, punto 2, i deployer che sono organismi di diritto pubblico o sono enti privati che forniscono servizi pubblici e i deployer di sistemi di IA ad alto rischio di cui all'allegato III, punto 5, lettere b) e c), effettuano una valutazione dell'impatto sui diritti fondamentali che l'uso di tale sistema può produrre. A tal fine, i deployer effettuano una valutazione che comprende gli elementi seguenti:
 - a) una descrizione dei processi del deployer in cui il sistema di IA ad alto rischio sarà utilizzato in linea con la sua finalità prevista;
 - b) una descrizione del periodo di tempo entro il quale ciascun sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza;

- c) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico;
 - d) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati a norma della lettera c), del presente paragrafo tenendo conto delle informazioni trasmesse dal fornitore a norma dell'articolo 13;
 - e) una descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso;
 - f) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo.
2. L'obbligo di cui al paragrafo 1 si applica al primo uso del sistema di IA ad alto rischio. Il deployer può, in casi analoghi, basarsi su valutazioni d'impatto sui diritti fondamentali effettuate in precedenza o su valutazioni d'impatto esistenti effettuate da un fornitore. Se, durante l'uso del sistema di IA ad alto rischio, ritiene che uno qualsiasi degli elementi elencati al paragrafo 1 sia cambiato o non sia più aggiornato, il deployer adotta le misure necessarie per aggiornare le informazioni.
3. Una volta effettuata la valutazione di cui al paragrafo 1 del presente articolo, il deployer notifica all'autorità di vigilanza del mercato i suoi risultati, presentando il modello compilato di cui al paragrafo 5 del presente articolo nell'ambito della notifica. Nel caso di cui all'articolo 46, paragrafo 1, i deployer possono essere esentati da tale obbligo di notifica.

4. Se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati.
5. L'ufficio per l'IA elabora un modello di questionario, anche attraverso uno strumento automatizzato, per agevolare i deployer nell'adempimento dei loro obblighi a norma del presente articolo in modo semplificato.

SEZIONE 4

AUTORITÀ DI NOTIFICA E ORGANISMI NOTIFICATI

Articolo 28

Autorità di notifica

1. Ciascuno Stato membro designa o istituisce almeno un'autorità di notifica responsabile della predisposizione e dell'esecuzione delle procedure necessarie per la valutazione, la designazione e la notifica degli organismi di valutazione della conformità e per il loro monitoraggio. Tali procedure sono sviluppate nell'ambito della collaborazione tra le autorità di notifica di tutti gli Stati membri.
2. Gli Stati membri possono decidere che la valutazione e il monitoraggio di cui al paragrafo 1 siano eseguiti da un organismo nazionale di accreditamento ai sensi e in conformità del regolamento (CE) n. 765/2008.

3. Le autorità di notifica sono istituite, organizzate e gestite in modo tale che non sorgano conflitti di interesse con gli organismi di valutazione della conformità e che siano salvaguardate l'obiettività e l'imparzialità delle loro attività.
4. Le autorità di notifica sono organizzate in modo che le decisioni relative alla notifica di un organismo di valutazione della conformità siano prese da persone competenti, diverse da quelle che hanno effettuato la valutazione.
5. Le autorità di notifica non offrono né svolgono alcuna delle attività eseguite dagli organismi di valutazione della conformità, né servizi di consulenza su base commerciale o concorrenziale.
6. Le autorità di notifica salvaguardano la riservatezza delle informazioni che ottengono conformemente all'articolo 78.
7. Le autorità di notifica dispongono di un numero adeguato di dipendenti competenti per l'adeguata esecuzione dei relativi compiti. I dipendenti competenti dispongono, se del caso, delle competenze necessarie per svolgere le proprie funzioni in settori quali le tecnologie dell'informazione, l'IA e il diritto, compreso il controllo dei diritti fondamentali.

Articolo 29

Domanda di notifica presentata dagli organismi di valutazione della conformità

1. Gli organismi di valutazione della conformità presentano una domanda di notifica all'autorità di notifica dello Stato membro in cui sono stabiliti.

2. La domanda di notifica è accompagnata da una descrizione delle attività di valutazione della conformità, del modulo o dei moduli di valutazione della conformità e dei tipi di sistemi di IA per i quali tale organismo di valutazione della conformità dichiara di essere competente, nonché da un certificato di accreditamento, se disponibile, rilasciato da un organismo nazionale di accreditamento che attesti che l'organismo di valutazione della conformità è conforme ai requisiti di cui all'articolo 31.

Sono aggiunti documenti validi relativi alle designazioni esistenti dell'organismo notificato richiedente ai sensi di qualsiasi altra normativa di armonizzazione dell'Unione.

3. Qualora non possa fornire un certificato di accreditamento, l'organismo di valutazione della conformità interessato fornisce all'autorità di notifica tutte le prove documentali necessarie per la verifica, il riconoscimento e il monitoraggio periodico della sua conformità ai requisiti di cui all'articolo 31.
4. Per gli organismi notificati designati ai sensi di qualsiasi altra normativa di armonizzazione dell'Unione, tutti i documenti e i certificati connessi a tali designazioni possono essere utilizzati a sostegno della loro procedura di designazione a norma del presente regolamento, a seconda dei casi. L'organismo notificato aggiorna la documentazione di cui ai paragrafi 2 e 3 del presente articolo ogni volta che si verificano cambiamenti di rilievo, al fine di consentire all'autorità responsabile degli organismi notificati di monitorare e verificare il continuo rispetto di tutte le prescrizioni di cui all'articolo 31.

Articolo 30
Procedura di notifica

1. Le autorità di notifica possono notificare solo gli organismi di valutazione della conformità che siano conformi alle prescrizioni di cui all'articolo 31.
2. Le autorità di notifica notificano alla Commissione e agli altri Stati membri, utilizzando lo strumento elettronico di notifica elaborato e gestito dalla Commissione, ogni organismo di valutazione della conformità di cui al paragrafo 1.
3. La notifica di cui al paragrafo 2 del presente articolo include tutti i dettagli riguardanti le attività di valutazione della conformità, il modulo o i moduli di valutazione della conformità, i tipi di sistemi di IA interessati, nonché la relativa attestazione di competenza. Qualora una notifica non sia basata su un certificato di accreditamento di cui all'articolo 29, paragrafo 2, l'autorità di notifica fornisce alla Commissione e agli altri Stati membri le prove documentali che attestino la competenza dell'organismo di valutazione della conformità nonché le misure predisposte per fare in modo che tale organismo sia monitorato periodicamente e continui a soddisfare i requisiti di cui all'articolo 31.
4. L'organismo di valutazione della conformità interessato può eseguire le attività di un organismo notificato solo se non sono sollevate obiezioni da parte della Commissione o degli altri Stati membri entro due settimane dalla notifica da parte di un'autorità di notifica, qualora essa includa un certificato di accreditamento di cui all'articolo 29, paragrafo 2, o entro due mesi dalla notifica da parte dell'autorità di notifica, qualora essa includa le prove documentali di cui all'articolo 29, paragrafo 3.

5. Se sono sollevate obiezioni, la Commissione avvia senza ritardo consultazioni con gli Stati membri pertinenti e l'organismo di valutazione della conformità. Tenutone debito conto, la Commissione decide se l'autorizzazione è giustificata. La Commissione trasmette la propria decisione allo Stato membro interessato e all'organismo di valutazione della conformità pertinente.

Articolo 31

Requisiti relativi agli organismi notificati

1. Un organismo notificato è istituito a norma del diritto nazionale di uno Stato membro e ha personalità giuridica.
2. Gli organismi notificati soddisfano i requisiti organizzativi, di gestione della qualità e relativi alle risorse e ai processi necessari all'assolvimento dei loro compiti nonché i requisiti idonei di cbersicurezza.
3. La struttura organizzativa, l'assegnazione delle responsabilità, le linee di riporto e il funzionamento degli organismi notificati garantiscono la fiducia nelle loro prestazioni e nei risultati delle attività di valutazione della conformità che essi effettuano.
4. Gli organismi notificati sono indipendenti dal fornitore di un sistema di IA ad alto rischio in relazione al quale svolgono attività di valutazione della conformità. Gli organismi notificati sono inoltre indipendenti da qualsiasi altro operatore avente un interesse economico nei sistemi di IA ad alto rischio oggetto della valutazione, nonché da eventuali concorrenti del fornitore. Ciò non preclude l'uso dei sistemi di IA ad alto rischio oggetto della valutazione che sono necessari per il funzionamento dell'organismo di valutazione della conformità o l'uso di tali sistemi di IA ad alto rischio per scopi privati.

5. L'organismo di valutazione della conformità, i suoi alti dirigenti e il personale incaricato di svolgere i compiti di valutazione della conformità non intervengono direttamente nella progettazione, nello sviluppo, nella commercializzazione o nell'utilizzo di sistemi di IA ad alto rischio, né rappresentano i soggetti impegnati in tali attività. Essi non intraprendono alcuna attività che possa essere in conflitto con la loro indipendenza di giudizio o la loro integrità per quanto riguarda le attività di valutazione della conformità per le quali sono notificati. Ciò vale in particolare per i servizi di consulenza.
6. Gli organismi notificati sono organizzati e gestiti in modo da salvaguardare l'indipendenza, l'obiettività e l'imparzialità delle loro attività. Gli organismi notificati documentano e attuano una struttura e procedure per salvaguardare l'imparzialità e per promuovere e applicare i principi di imparzialità in tutta l'organizzazione, tra il personale e nelle attività di valutazione.
7. Gli organismi notificati dispongono di procedure documentate per garantire che il loro personale, i loro comitati, le affiliate, i subappaltatori e qualsiasi altra organizzazione associata o il personale di organismi esterni mantengano, conformemente all'articolo 78, la riservatezza delle informazioni di cui vengono in possesso nello svolgimento delle attività di valutazione della conformità, salvo quando la normativa ne prescriva la divulgazione. Il personale degli organismi notificati è tenuto a osservare il segreto professionale riguardo a tutte le informazioni ottenute nello svolgimento dei propri compiti a norma del presente regolamento, tranne che nei confronti delle autorità di notifica dello Stato membro in cui svolge le proprie attività.

8. Gli organismi notificati dispongono di procedure per svolgere le attività che tengono debitamente conto delle dimensioni di un fornitore, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA interessato.
9. Gli organismi notificati sottoscrivono un'adeguata assicurazione di responsabilità per le loro attività di valutazione della conformità, a meno che lo Stato membro in cui sono stabiliti non si assuma tale responsabilità a norma del diritto nazionale o non sia esso stesso direttamente responsabile della valutazione della conformità.
10. Gli organismi notificati sono in grado di eseguire tutti i compiti assegnati loro in forza del presente regolamento con il più elevato grado di integrità professionale e di competenza richiesta nel settore specifico, indipendentemente dal fatto che tali compiti siano eseguiti dagli organismi notificati stessi o per loro conto e sotto la loro responsabilità.
11. Gli organismi notificati dispongono di sufficienti competenze interne per poter valutare efficacemente i compiti svolti da parti esterne per loro conto. Gli organismi notificati dispongono permanentemente di sufficiente personale amministrativo, tecnico, giuridico e scientifico dotato di esperienza e conoscenze relative ai tipi di sistemi di IA, ai dati, al calcolo dei dati pertinenti, nonché ai requisiti di cui alla sezione 2.
12. Gli organismi notificati partecipano alle attività di coordinamento di cui all'articolo 38. Inoltre essi partecipano direttamente o sono rappresentati in seno alle organizzazioni europee di normazione o garantiscono di essere informati e di mantenersi aggiornati in merito alle norme pertinenti.

Articolo 32

Presunzione di conformità ai requisiti relativi agli organismi notificati

Qualora dimostri la propria conformità ai criteri stabiliti nelle pertinenti norme armonizzate o in parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*, l'organismo di valutazione della conformità è considerato conforme ai requisiti di cui all'articolo 31 nella misura in cui le norme armonizzate applicabili coprano tali requisiti.

Articolo 33

Affiliate degli organismi notificati e subappaltatori

1. L'organismo notificato, qualora subappalti compiti specifici connessi alla valutazione della conformità oppure ricorra a un'affiliata, garantisce che il subappaltatore o l'affiliata soddisfino i requisiti di cui all'articolo 31 e ne informa l'autorità di notifica.
2. Gli organismi notificati si assumono la completa responsabilità dei compiti eseguiti da eventuali subappaltatori o affiliate.
3. Le attività possono essere subappaltate o eseguite da un'affiliata solo con il consenso del fornitore. Gli organismi notificati mettono a disposizione del pubblico un elenco delle loro affiliate.
4. I documenti pertinenti riguardanti la valutazione delle qualifiche del subappaltatore o dell'affiliata e il lavoro da essi eseguito a norma del presente regolamento sono tenuti a disposizione dell'autorità di notifica per un periodo di cinque anni a decorrere dalla data in cui termina il contratto di subappalto.

Articolo 34

Obblighi operativi degli organismi notificati

1. Gli organismi notificati verificano la conformità dei sistemi di IA ad alto rischio secondo le procedure di valutazione della conformità di cui all'articolo 43.
2. Gli organismi notificati evitano oneri inutili per i fornitori nello svolgimento delle loro attività e tengono debitamente conto delle dimensioni del fornitore, del settore in cui opera, della sua struttura e del grado di complessità del sistema di IA ad alto rischio interessato, in particolare al fine di ridurre al minimo gli oneri amministrativi e i costi di conformità per le microimprese e le piccole imprese ai sensi della raccomandazione 2003/361/CE.
L'organismo notificato rispetta tuttavia il grado di rigore e il livello di tutela necessari per la conformità del sistema di IA ad alto rischio rispetto ai requisiti del presente regolamento.
3. Gli organismi notificati mettono a disposizione e trasmettono su richiesta tutta la documentazione pertinente, inclusa la documentazione del fornitore, all'autorità di notifica di cui all'articolo 28 per consentirle di svolgere le proprie attività di valutazione, designazione, notifica e monitoraggio e per agevolare la valutazione di cui alla presente sezione.

Articolo 35

Numeri di identificazione ed elenchi di organismi notificati

1. La Commissione assegna un numero di identificazione unico a ciascun organismo notificato, anche se un organismo è notificato a norma di più atti dell'Unione.

2. La Commissione mette pubblicamente a disposizione l'elenco degli organismi notificati ai sensi del presente regolamento, inclusi i loro numeri di identificazione e le attività per le quali sono stati notificati. La Commissione garantisce che l'elenco sia tenuto aggiornato.

Articolo 36

Modifiche delle notifiche

1. L'autorità di notifica informa la Commissione e gli altri Stati membri di ogni pertinente modifica della notifica di un organismo notificato tramite lo strumento elettronico di notifica di cui all'articolo 30, paragrafo 2.
2. Le procedure di cui agli articoli 29 e 30 si applicano alle estensioni della portata della notifica.

In caso di modifiche della notifica diverse dalle estensioni della sua portata, si applicano le procedure stabilite nei paragrafi da 3 a 9.

3. Qualora decida di cessare le attività di valutazione della conformità, un organismo notificato ne informa l'autorità di notifica e i fornitori interessati quanto prima possibile e almeno un anno prima della cessazione delle attività qualora la cessazione sia stata programmata. I certificati dell'organismo notificato possono restare validi per un periodo di nove mesi dopo la cessazione delle attività dell'organismo notificato purché un altro organismo notificato abbia confermato per iscritto che assumerà la responsabilità per i sistemi di IA ad alto rischio coperti da tale certificato. Quest'ultimo organismo notificato completa una valutazione integrale dei sistemi di IA ad alto rischio coinvolti entro la fine del periodo di nove mesi indicato prima di rilasciare nuovi certificati per gli stessi sistemi. Qualora l'organismo notificato abbia cessato le proprie attività, l'autorità di notifica ritira la designazione.

4. Qualora un'autorità di notifica abbia motivo sufficiente di ritenere che un organismo notificato non soddisfa più i requisiti di cui all'articolo 31 o non adempie i suoi obblighi, l'autorità di notifica indaga senza ritardo sulla questione con la massima diligenza. In tale contesto, essa informa l'organismo notificato interessato in merito alle obiezioni sollevate e gli dà la possibilità di esprimere il suo punto di vista. Se l'autorità di notifica conclude che l'organismo notificato non soddisfa più i requisiti di cui all'articolo 31 o non adempie i suoi obblighi, tale autorità limita, sospende o ritira la designazione, a seconda dei casi, in funzione della gravità del mancato rispetto di tali requisiti o dell'inadempimento di tali obblighi. Essa informa immediatamente la Commissione e gli altri Stati membri.
5. Qualora la sua designazione sia stata sospesa, limitata oppure ritirata interamente o in parte, l'organismo notificato informa i fornitori interessati al più tardi entro 10 giorni.
6. In caso di limitazione, sospensione o ritiro di una designazione, l'autorità di notifica adotta le misure appropriate per far sì che i fascicoli dell'organismo notificato interessato siano conservati e messi a disposizione delle autorità di notifica in altri Stati membri nonché delle autorità di vigilanza del mercato, su richiesta.
7. In caso di limitazione, sospensione o ritiro di una designazione, l'autorità di notifica:
 - a) valuta l'impatto sui certificati rilasciati dall'organismo notificato;
 - b) entro tre mesi dalla comunicazione delle modifiche della designazione, presenta alla Commissione e agli altri Stati membri una relazione sulle proprie constatazioni;

- c) impone all'organismo notificato di sospendere o ritirare, entro un periodo di tempo ragionevole stabilito dall'autorità, i certificati rilasciati indebitamente al fine di garantire la continua conformità dei sistemi di IA ad alto rischio sul mercato;
- d) informa la Commissione e gli Stati membri in merito ai certificati di cui ha richiesto la sospensione o il ritiro;
- e) fornisce alle autorità nazionali competenti dello Stato membro in cui ha sede il fornitore tutte le informazioni pertinenti sui certificati di cui ha richiesto la sospensione o il ritiro; tale autorità adotta le misure appropriate, laddove necessario, per evitare un rischio potenziale per la salute, la sicurezza o i diritti fondamentali.

8. Ad eccezione dei certificati rilasciati indebitamente, e ove la designazione sia stata sospesa o limitata, i certificati restano validi in uno dei casi seguenti:

- a) l'autorità di notifica ha confermato, entro un mese dalla sospensione o dalla limitazione, che sotto il profilo della salute, della sicurezza o dei diritti fondamentali non sussistono rischi per quanto riguarda i certificati oggetto di sospensione o limitazione e l'autorità di notifica ha predisposto un calendario di azioni al fine di porre rimedio alla sospensione o alla limitazione; oppure

- b) l'autorità di notifica ha confermato che durante il periodo di sospensione o di limitazione non saranno rilasciati, modificati o rinnovati certificati attinenti alla sospensione e indica se l'organismo notificato è in grado di continuare a svolgere il monitoraggio e rimanere responsabile dei certificati esistenti rilasciati durante il periodo della sospensione o della limitazione; nel caso in cui l'autorità di notifica stabilisca che l'organismo notificato non è in grado di sostenere i certificati in vigore, il fornitore del sistema coperto dal certificato conferma per iscritto alle autorità nazionali competenti dello Stato membro in cui ha la propria sede, entro tre mesi dalla sospensione o dalla limitazione, che un altro organismo notificato qualificato assume temporaneamente le funzioni dell'organismo notificato di svolgere il monitoraggio e assume la responsabilità dei certificati durante il periodo di sospensione o limitazione.

9. Ad eccezione dei certificati rilasciati indebitamente, e ove la designazione sia stata ritirata, i certificati restano validi per un periodo di nove mesi nei casi seguenti:

- a) l'autorità nazionale competente dello Stato membro in cui il fornitore del sistema di IA ad alto rischio coperto dal certificato ha la propria sede ha confermato che sotto il profilo della salute, della sicurezza o dei diritti fondamentali non sussistono rischi per quanto riguarda i sistemi di IA ad alto rischio interessati; e
- b) un altro organismo notificato ha confermato per iscritto che assume immediatamente la responsabilità per tali sistemi di IA e completa la sua valutazione entro 12 mesi dal ritiro della designazione.

Nei casi di cui al primo comma, l'autorità nazionale competente dello Stato membro in cui il fornitore del sistema coperto dal certificato ha la propria sede può prorogare la validità temporanea dei certificati di ulteriori periodi di tre mesi, per un totale non superiore a dodici mesi.

L'autorità nazionale competente o l'organismo notificato che assume le funzioni dell'organismo notificato interessato dalla modifica della designazione informa immediatamente la Commissione, gli altri Stati membri e gli altri organismi notificati.

Articolo 37

Contestazione della competenza degli organismi notificati

1. Ove necessario, la Commissione indaga su tutti i casi in cui vi siano motivi di dubitare della competenza di un organismo notificato o della continuità dell'ottemperanza di un organismo notificato ai requisiti di cui all'articolo 31 e alle sue responsabilità applicabili.
2. L'autorità di notifica fornisce alla Commissione, su richiesta, tutte le informazioni relative alla notifica o al mantenimento della competenza dell'organismo notificato interessato.
3. La Commissione provvede affinché tutte le informazioni sensibili ottenute nel corso delle sue indagini a norma del presente articolo siano trattate in maniera riservata in conformità dell'articolo 78.

4. La Commissione, qualora accerti che un organismo notificato non soddisfa, o non soddisfa più, i requisiti per la sua notifica, informa di conseguenza lo Stato membro notificante e gli chiede di adottare le misure correttive necessarie compresa la sospensione o il ritiro della notifica. Se lo Stato membro non adotta le misure correttive necessarie, la Commissione può, mediante atto di esecuzione, sospendere, limitare o ritirare la designazione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Articolo 38

Coordinamento degli organismi notificati

1. La Commissione garantisce che, per quanto riguarda i sistemi di IA ad alto rischio, siano istituiti e funzionino correttamente, in forma di gruppo settoriale di organismi notificati, un coordinamento e una cooperazione adeguati tra gli organismi notificati che partecipano alle procedure di valutazione della conformità a norma del presente regolamento.
2. Ciascuna autorità di notifica garantisce che gli organismi da essa notificati partecipino al lavoro di un gruppo di cui al paragrafo 1, direttamente o mediante rappresentanti designati.
3. La Commissione provvede allo scambio di conoscenze e migliori pratiche tra le autorità di notifica.

Articolo 39

Organismi di valutazione della conformità di paesi terzi

Gli organismi di valutazione della conformità istituiti a norma del diritto di un paese terzo con il quale l'Unione ha concluso un accordo possono essere autorizzati a svolgere le attività degli organismi notificati a norma del presente regolamento, a condizione che soddisfino i requisiti stabiliti all'articolo 31 o garantiscano un livello di conformità equivalente.

SEZIONE 5

NORME, VALUTAZIONE DELLA CONFORMITÀ, CERTIFICATI, REGISTRAZIONE

Articolo 40

Norme armonizzate e prodotti della normazione

1. I sistemi di IA ad alto rischio o i modelli di IA per finalità generali che sono conformi alle norme armonizzate o a parti di esse i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n. 1025/2012 si presumono conformi ai requisiti di cui alla sezione 2 del presente capo o, se del caso, agli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento, nella misura in cui tali requisiti o obblighi sono contemplati da tali norme.

2. In conformità dell'articolo 10 del regolamento (UE) n. 1025/2012, la Commissione presenta senza indebito ritardo richieste di normazione riguardanti tutti i requisiti di cui alla sezione 2 del presente capo e, se del caso, richieste di normazione riguardanti gli obblighi di cui al capo V, sezioni 2 e 3, del presente regolamento. La richiesta di normazione chiede inoltre prodotti relativi a processi di comunicazione e documentazione intesi a migliorare le prestazioni dei sistemi di IA in termini di risorse, come la riduzione del consumo di energia e di altre risorse del sistema di IA ad alto rischio durante il suo ciclo di vita, e allo sviluppo efficiente sotto il profilo energetico dei modelli di IA per finalità generali. Nel preparare una richiesta di normazione, la Commissione consulta il consiglio per l'IA e i pertinenti portatori di interessi, compreso il forum consultivo.

Nel presentare una richiesta di normazione alle organizzazioni europee di normazione, la Commissione specifica che le norme devono essere chiare, coerenti, anche con le norme elaborate nei vari settori per i prodotti disciplinati dalla vigente normativa di armonizzazione dell'Unione elencata nell'allegato I, e volte a garantire che i sistemi di IA ad alto rischio o i modelli di IA per finalità generali immessi sul mercato o messi in servizio nell'Unione soddisfino i pertinenti requisiti od obblighi di cui al presente regolamento.

La Commissione chiede alle organizzazioni europee di normazione di dimostrare che si adoperano al massimo per conseguire gli obiettivi di cui al primo e al secondo comma del presente paragrafo conformemente all'articolo 24 del regolamento (UE) n. 1025/2012.

3. I partecipanti al processo di normazione cercano di promuovere gli investimenti e l'innovazione nell'IA, anche mediante una maggiore certezza del diritto, nonché la competitività e la crescita del mercato dell'Unione, di contribuire a rafforzare la cooperazione globale in materia di normazione e a tener conto delle norme internazionali esistenti nel settore dell'IA che sono coerenti con i valori, i diritti fondamentali e gli interessi dell'Unione, e di rafforzare la governance multipartecipativa garantendo una rappresentanza equilibrata degli interessi e l'effettiva partecipazione di tutti i portatori di interessi pertinenti conformemente agli articoli 5, 6 e 7 del regolamento (UE) n. 1025/2012.

Articolo 41

Specifiche comuni

1. La Commissione può adottare atti di esecuzione che stabiliscano specifiche comuni per i requisiti di cui alla sezione 2 del presente capo o, se del caso, per gli obblighi di cui al capo V, sezioni 2 e 3, se sono soddisfatte le condizioni seguenti:
- a) a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012, la Commissione ha chiesto a una o più organizzazioni europee di normazione di elaborare una norma armonizzata per i requisiti di cui alla sezione 2 del presente capo, o ove applicabile, per gli obblighi di cui al capo V, sezioni 2 e 3, e:
 - i) la richiesta non è stata accettata da nessuna delle organizzazioni europee di normazione; o

- ii) le norme armonizzate relative a tale richiesta non vengono presentate entro il termine fissato a norma dell'articolo 10, paragrafo 1, del regolamento (UE) n. 1025/2012; o
 - iii) le pertinenti norme armonizzate non tengono sufficientemente conto delle preoccupazioni in materia di diritti fondamentali; o
 - iv) le norme armonizzate non sono conformi alla richiesta; e
- b) nessun riferimento a norme armonizzate, che contemplino i requisiti di cui alla sezione 2 del presente capo o, ove applicabile, gli obblighi di cui al capo V, sezioni 2 e 3, è stato pubblicato nella *Gazzetta ufficiale dell'Unione europea* conformemente al regolamento (UE) n. 1025/2012 e non si prevede che un tale riferimento sia pubblicato entro un termine ragionevole.

Nel redigere le specifiche comuni, la Commissione consulta il forum consultivo di cui all'articolo 67.

Gli atti di esecuzione di cui al primo comma sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

2. Prima di preparare un progetto di atto di esecuzione, la Commissione informa il comitato di cui all'articolo 22 del regolamento (UE) n. 1025/2012 del fatto che ritiene soddisfatte le condizioni di cui al paragrafo 1 del presente articolo.

3. I sistemi di IA ad alto rischio o i modelli di IA per finalità generali conformi alle specifiche comuni di cui al paragrafo 1, o a parti di tali specifiche, si presumono conformi ai requisiti di cui alla sezione 2 del presente capo o, ove applicabile, agli obblighi di cui al capo V, sezioni 2 e 3 nella misura in cui tali requisiti o tali obblighi sono contemplati da tali specifiche comuni.
4. Qualora una norma armonizzata sia adottata da un organismo europeo di normazione e proposta alla Commissione per la pubblicazione del suo riferimento nella *Gazzetta ufficiale dell'Unione europea*, la Commissione valuta la norma armonizzata conformemente al regolamento (UE) n. 1025/2012. Quando un riferimento a una norma armonizzata è pubblicato nella *Gazzetta ufficiale dell'Unione europea*, la Commissione abroga gli atti di esecuzione di cui al paragrafo 1 o le parti di tali atti che riguardano gli stessi requisiti di cui alla sezione 2 del presente capo o, ove applicabile, gli obblighi di cui al capo V, sezioni 2 e 3.
5. Qualora non rispettino le specifiche comuni di cui al paragrafo 1, i fornitori di sistemi di IA ad alto rischio o di modelli di IA per finalità generali adottano soluzioni tecniche debitamente motivate che soddisfano i requisiti di cui alla sezione 2 del presente capo o, ove applicabile, gli obblighi di cui al capo V, sezioni 2 e 3, a un livello almeno equivalente.

6. Se uno Stato membro ritiene che una specifica comune non soddisfi interamente i requisiti di cui alla sezione 2 o, ove applicabile, non rispetti gli obblighi di cui al capo V, sezioni 2 e 3, ne informa la Commissione fornendo una spiegazione dettagliata. La Commissione valuta tali informazioni e, ove necessario, modifica l'atto di esecuzione che stabilisce la specifica comune interessata.

Articolo 42

Presunzione di conformità a determinati requisiti

1. I sistemi di IA ad alto rischio che sono stati addestrati e sottoposti a prova con dati che rispecchiano il contesto geografico, comportamentale, contestuale o funzionale specifico all'interno del quale sono destinati a essere usati si presumono conformi ai pertinenti requisiti di cui all'articolo 10, paragrafo 4.
2. I sistemi di IA ad alto rischio che sono stati certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cibersecurity a norma del regolamento (UE) 2019/881 e i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea* si presumono conformi ai requisiti di cibersecurity di cui all'articolo 15 del presente regolamento, nella misura in cui tali requisiti siano contemplati nel certificato di cibersecurity o nella dichiarazione di conformità o in parti di essi.

Articolo 43
Valutazione della conformità

1. Per i sistemi di IA ad alto rischio elencati nell'allegato III, punto 1, se ha applicato le norme armonizzate di cui all'articolo 40 o, ove applicabile, le specifiche comuni di cui all'articolo 41, nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, il fornitore sceglie una delle seguenti procedure di valutazione della conformità basate sugli elementi qui di seguito:

- a) il controllo interno di cui all'allegato VI; oppure
- b) la valutazione del sistema di gestione della qualità e la valutazione della documentazione tecnica, con il coinvolgimento di un organismo notificato, di cui all'allegato VII.

Nel dimostrare la conformità di un sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, il fornitore segue la procedura di valutazione della conformità di cui all'allegato VII se:

- a) non esistono le norme armonizzate di cui all'articolo 40 e non sono disponibili le specifiche comuni di cui all'articolo 41;
- b) il fornitore non ha applicato la norma armonizzata o ne ha applicato solo una parte;
- c) esistono le specifiche comuni di cui alla lettera a), ma il fornitore non le ha applicate;

- d) una o più norme armonizzate di cui alla lettera a) sono state pubblicate con una limitazione e soltanto sulla parte della norma che è oggetto di limitazione.

Ai fini della procedura di valutazione della conformità di cui all'allegato VII, il fornitore può scegliere uno qualsiasi degli organismi notificati. Tuttavia, se il sistema di IA ad alto rischio è destinato ad essere messo in servizio dalle autorità competenti in materia di contrasto, di immigrazione o di asilo, nonché da istituzioni, organi o organismi dell'Unione, l'autorità di vigilanza del mercato di cui all'articolo 74, paragrafo 8 o 9, a seconda dei casi, agisce in qualità di organismo notificato.

2. Per i sistemi di IA ad alto rischio di cui all'allegato III, punti da 2 a 8, i fornitori seguono la procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI, che non prevede il coinvolgimento di un organismo notificato.
3. Per i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, il fornitore segue la pertinente procedura di valutazione della conformità prevista da tali atti giuridici. I requisiti di cui alla sezione 2 del presente capo si applicano a tali sistemi di IA ad alto rischio e fanno parte di tale valutazione. Si applicano anche i punti 4.3, 4.4, 4.5 e il punto 4.6, quinto comma, dell'allegato VII.

Ai fini di tale valutazione, gli organismi notificati che sono stati notificati a norma di tali atti giuridici hanno la facoltà di controllare la conformità dei sistemi di IA ad alto rischio ai requisiti di cui alla sezione 2, a condizione che la conformità di tali organismi notificati ai requisiti di cui all'articolo 31, paragrafi 4, 10 e 11, sia stata valutata nel contesto della procedura di notifica a norma di tali atti giuridici.

Qualora un atto giuridico elencato nell'allegato I, sezione A, consenta al fabbricante del prodotto di sottrarsi a una valutazione della conformità da parte di terzi, purché abbia applicato tutte le norme armonizzate che contemplano tutti i requisiti pertinenti, tale fabbricante può avvalersi di tale facoltà solo se ha applicato anche le norme armonizzate o, ove applicabili, le specifiche comuni di cui all'articolo 41, che contemplano tutti i requisiti di cui alla sezione 2 del presente capo.

4. I sistemi di IA ad alto rischio che sono già stati oggetto di una procedura di valutazione della conformità sono sottoposti a una nuova procedura di valutazione della conformità nel caso di una modifica sostanziale, indipendentemente dal fatto che il sistema modificato sia destinato a essere ulteriormente distribuito o continui a essere usato dal deployer attuale.

Per i sistemi di IA ad alto rischio che proseguono il loro apprendimento dopo essere stati immessi sul mercato o messi in servizio, le modifiche apportate al sistema di IA ad alto rischio e alle sue prestazioni che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità e fanno parte delle informazioni contenute nella documentazione tecnica di cui all'allegato IV, punto 2, lettera f), non costituiscono una modifica sostanziale.

5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare gli allegati VI e VII aggiornandoli alla luce del progresso tecnico.

6. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 che modificano i paragrafi 1 e 2 del presente articolo per assoggettare i sistemi di IA ad alto rischio di cui all'allegato III, punti da 2 a 8, alla procedura di valutazione della conformità di cui all'allegato VII o a parti di essa. La Commissione adotta tali atti delegati tenendo conto dell'efficacia della procedura di valutazione della conformità basata sul controllo interno di cui all'allegato VI nel prevenire o ridurre al minimo i rischi per la salute, la sicurezza e la protezione dei diritti fondamentali posti da tali sistemi, nonché della disponibilità di capacità e risorse adeguate tra gli organismi notificati.

Articolo 44

Certificati

1. I certificati rilasciati dagli organismi notificati a norma dell'allegato VII sono redatti in una lingua che può essere facilmente compresa dalle autorità pertinenti dello Stato membro in cui è stabilito l'organismo notificato.
2. I certificati sono validi per il periodo da essi indicato che non supera i cinque anni per i sistemi di IA disciplinati dall'allegato I e i quattro anni per i sistemi di IA disciplinati dall'allegato III. Su domanda del fornitore, la validità di un certificato può essere prorogata per ulteriori periodi, ciascuno non superiore a cinque anni per i sistemi di IA disciplinati dall'allegato I e a quattro anni per i sistemi di IA disciplinati dall'allegato III, sulla base di una nuova valutazione secondo le procedure di valutazione della conformità applicabili. Ogni supplemento del certificato rimane valido purché sia valido il certificato cui si riferisce.

3. Qualora constati che il sistema di IA non soddisfa più i requisiti di cui alla sezione 2, l'organismo notificato, tenendo conto del principio di proporzionalità, sospende o ritira il certificato rilasciato o impone limitazioni, a meno che la conformità a tali requisiti sia garantita mediante opportune misure correttive adottate dal fornitore del sistema entro un termine adeguato stabilito dall'organismo notificato. L'organismo notificato motiva la propria decisione.

È disponibile una procedura di ricorso contro le decisioni degli organismi notificati, anche sui certificati di conformità rilasciati.

Articolo 45

Obblighi di informazione degli organismi notificati

1. Gli organismi notificati informano l'autorità di notifica in merito a quanto segue:
- a) i certificati di valutazione della documentazione tecnica dell'Unione, i supplementi a tali certificati e le approvazioni dei sistemi di gestione della qualità rilasciati in conformità dei requisiti dell'allegato VII;
 - b) qualsiasi rifiuto, limitazione, sospensione o ritiro di un certificato di valutazione della documentazione tecnica dell'Unione o un'approvazione del sistema di gestione della qualità rilasciati in conformità dei requisiti dell'allegato VII;
 - c) qualsiasi circostanza che influisca sull'ambito o sulle condizioni della notifica;

- d) qualsiasi richiesta di informazioni che abbiano ricevuto dalle autorità di vigilanza del mercato, in relazione ad attività di valutazione della conformità;
 - e) su richiesta, le attività di valutazione della conformità effettuate nell'ambito della loro notifica e qualsiasi altra attività, incluse quelle transfrontaliere e il subappalto.
2. Ciascun organismo notificato informa gli altri organismi notificati in merito a quanto segue:
- a) le approvazioni dei sistemi di gestione della qualità da esso rifiutate, sospese o ritirate e, su richiesta, le approvazioni dei sistemi di qualità da esso rilasciate;
 - b) i certificati di valutazione della documentazione tecnica dell'Unione o i relativi supplementi da esso rifiutati, ritirati, sospesi o altrimenti limitati e, su richiesta, i certificati e/o i relativi supplementi da esso rilasciati.
3. Ciascun organismo notificato fornisce agli altri organismi notificati che svolgono attività simili di valutazione della conformità riguardanti gli stessi tipi di sistemi di IA informazioni pertinenti su questioni relative ai risultati negativi e, su richiesta, positivi della valutazione della conformità.
4. Gli organismi notificati tutelano la riservatezza delle informazioni che ottengono in conformità dell'articolo 78.

Articolo 46

Deroga alla procedura di valutazione della conformità

1. In deroga all'articolo 43 e su richiesta debitamente giustificata, qualsiasi autorità di vigilanza del mercato può autorizzare l'immissione sul mercato o la messa in servizio di specifici sistemi di IA ad alto rischio nel territorio dello Stato membro interessato, per motivi eccezionali di sicurezza pubblica o di protezione della vita e della salute delle persone e di protezione dell'ambiente o dei principali beni industriali e infrastrutturali. Tale autorizzazione è valida per un periodo limitato, mentre sono in corso le necessarie procedure di valutazione della conformità, tenendo conto dei motivi eccezionali che giustificano la deroga. Il completamento di tali procedure è effettuato senza indebito ritardo.
2. In una situazione di urgenza debitamente giustificata per motivi eccezionali di sicurezza pubblica o in caso di minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche, le autorità di contrasto o le autorità di protezione civile possono mettere in servizio uno specifico sistema di IA ad alto rischio senza l'autorizzazione di cui al paragrafo 1, a condizione che tale autorizzazione sia richiesta durante o dopo l'uso senza indebito ritardo. Se l'autorizzazione di cui al paragrafo 1 è rifiutata, l'uso del sistema di IA ad alto rischio è interrotto con effetto immediato e tutti i risultati e gli output di tale uso sono immediatamente eliminati.

3. L'autorizzazione di cui al paragrafo 1 è rilasciata solo se l'autorità di vigilanza del mercato conclude che il sistema di IA ad alto rischio è conforme ai requisiti di cui alla sezione 2. L'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri di eventuali autorizzazioni rilasciate a norma dei paragrafi 1 e 2. Tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità di contrasto.
4. Se, entro 15 giorni di calendario dal ricevimento dell'informazione di cui al paragrafo 3, né gli Stati membri né la Commissione sollevano obiezioni in merito a un'autorizzazione rilasciata da un'autorità di vigilanza del mercato di uno Stato membro in conformità del paragrafo 1, tale autorizzazione è considerata giustificata.
5. Se, entro 15 giorni di calendario dal ricevimento della notifica di cui al paragrafo 3, uno Stato membro solleva obiezioni in merito a un'autorizzazione rilasciata da un'autorità di vigilanza del mercato di un altro Stato membro, o se la Commissione ritiene che l'autorizzazione sia contraria al diritto dell'Unione o che la conclusione degli Stati membri riguardante la conformità del sistema di cui al paragrafo 3 sia infondata, la Commissione avvia senza ritardo consultazioni con lo Stato membro interessato. Gli operatori interessati sono consultati e hanno la possibilità di esprimere il loro parere. Tenuto conto di ciò, la Commissione decide se l'autorizzazione è giustificata. La Commissione trasmette la propria decisione allo Stato membro interessato e agli operatori pertinenti.
6. Se la Commissione ritiene l'autorizzazione ingiustificata, essa è ritirata dall'autorità di vigilanza del mercato dello Stato membro interessato.

7. Per i sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, si applicano solo le deroghe alla valutazione della conformità stabilite in tale normativa di armonizzazione dell'Unione.

Articolo 47

Dichiarazione di conformità UE

1. Il fornitore compila una dichiarazione scritta di conformità UE leggibile meccanicamente, firmata a mano o elettronicamente, per ciascun sistema di IA ad alto rischio e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio. La dichiarazione di conformità UE identifica il sistema di IA ad alto rischio per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è presentata alle pertinenti autorità nazionali competenti.
2. La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio interessato soddisfa i requisiti di cui alla sezione 2. La dichiarazione di conformità UE riporta le informazioni di cui all'allegato V ed è tradotta in una lingua che può essere facilmente compresa dalle autorità nazionali competenti degli Stati membri nei quali il sistema di IA ad alto rischio è immesso sul mercato o messo a disposizione.

3. Qualora i sistemi di IA ad alto rischio siano soggetti ad altra normativa di armonizzazione dell'Unione che richieda anch'essa una dichiarazione di conformità UE, è redatta un'unica dichiarazione di conformità UE in relazione a tutte le normative dell'Unione applicabili al sistema di IA ad alto rischio. La dichiarazione contiene tutte le informazioni necessarie per identificare la normativa di armonizzazione dell'Unione cui si riferisce la dichiarazione.
4. Redigendo la dichiarazione di conformità UE, il fornitore si assume la responsabilità della conformità ai requisiti di cui alla sezione 2. Il fornitore tiene opportunamente aggiornata la dichiarazione di conformità UE.
5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato V aggiornando il contenuto della dichiarazione di conformità UE di cui a tale allegato per introdurre elementi che si rendano necessari alla luce del progresso tecnico.

Articolo 48

Marcatura CE

1. La marcatura CE è soggetta ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.
2. Per i sistemi di IA ad alto rischio forniti digitalmente è utilizzata una marcatura CE digitale soltanto se è facilmente accessibile attraverso l'interfaccia da cui si accede a tale sistema o tramite un codice leggibile meccanicamente o altri mezzi elettronici facilmente accessibili.

3. La marcatura CE è apposta sul sistema di IA ad alto rischio in modo visibile, leggibile e indelebile. Qualora ciò sia impossibile o difficilmente realizzabile a causa della natura del sistema di IA ad alto rischio, il marchio è apposto sull'imballaggio o sui documenti di accompagnamento, a seconda dei casi.
4. Ove applicabile, la marcatura CE è seguita dal numero di identificazione dell'organismo notificato responsabile delle procedure di valutazione della conformità di cui all'articolo 43. Il numero di identificazione dell'organismo notificato è apposto dall'organismo stesso o, in base alle istruzioni di quest'ultimo, dal fornitore o dal rappresentante autorizzato del fornitore. Il numero d'identificazione è inoltre indicato in tutto il materiale promozionale in cui si afferma che il sistema di IA ad alto rischio soddisfa i requisiti per la marcatura CE.
5. Se i sistemi di IA ad alto rischio sono disciplinati da altre disposizioni del diritto dell'Unione che prevedono anch'esse l'apposizione della marcatura CE, quest'ultima indica che i sistemi di IA ad alto rischio soddisfano anche i requisiti delle altre normative in questione.

Articolo 49

Registrazione

1. Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, il fornitore o, ove applicabile, il rappresentante autorizzato si registra e registra il suo sistema nella banca dati dell'UE di cui all'articolo 71.

2. Prima di immettere sul mercato o mettere in servizio un sistema di IA che il fornitore ha concluso non essere ad alto rischio a norma dell'articolo 6, paragrafo 3, il fornitore o, ove applicabile, il rappresentante autorizzato si registra o registra tale sistema nella banca dati dell'UE di cui all'articolo 71.
3. Prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi di IA ad alto rischio elencati nel punto 2 dell'allegato III, i deployer che sono autorità pubbliche, istituzioni, organi e organismi dell'Unione o persone che agiscono per loro conto si registrano, selezionano il sistema e ne registrano l'uso nella banca dati dell'UE di cui all'articolo 71.
4. Per i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, la registrazione di cui ai paragrafi 1, 2 e 3 del presente articolo si trova in una sezione sicura non pubblica della banca dati dell'UE di cui all'articolo 71 e comprende, a seconda dei casi, solo le informazioni seguenti di cui:
 - a) all'allegato VIII, sezione A, punti da 1 a 5 e punti 8 e 9;
 - b) all'allegato VIII, sezione B, punti da 1 a 5 e punti 8 e 9;
 - c) all'allegato VIII, sezione C, punti da 1 a 3;
 - d) all'allegato IX, punti 1, 2, 3 e 5.

Solo la Commissione e le autorità nazionali di cui all'articolo 74, paragrafo 8, hanno accesso alle rispettive sezioni riservate della banca dati dell'UE elencate al primo comma del presente paragrafo.

5. I sistemi di IA ad alto rischio di cui all'allegato III, punto 2, sono registrati a livello nazionale.

Capo IV

Obblighi di trasparenza per i fornitori e i deployer di determinati sistemi di IA

Articolo 50

Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA

1. I fornitori garantiscono che i sistemi di IA destinati a interagire direttamente con le persone fisiche sono progettati e sviluppati in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA, a meno che ciò non risulti evidente dal punto di vista di una persona fisica ragionevolmente informata, attenta e avveduta, tenendo conto delle circostanze e del contesto di utilizzo. Tale obbligo non si applica ai sistemi di IA autorizzati dalla legge per accertare, prevenire, indagare o perseguire reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi, a meno che tali sistemi non siano a disposizione del pubblico per segnalare un reato.

2. I fornitori di sistemi di IA, compresi i sistemi di IA per finalità generali, che generano contenuti audio, immagine, video o testuali sintetici, garantiscono che gli output del sistema di IA siano marcati in un formato leggibile meccanicamente e rilevabili come generati o manipolati artificialmente. I fornitori garantiscono che le loro soluzioni tecniche siano efficaci, interoperabili, solide e affidabili nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle specificità e dei limiti dei vari tipi di contenuti, dei costi di attuazione e dello stato dell'arte generalmente riconosciuto, come eventualmente indicato nelle pertinenti norme tecniche. Tale obbligo non si applica se i sistemi di IA svolgono una funzione di assistenza per l'editing standard o non modificano in modo sostanziale i dati di input forniti dal deployer o la rispettiva semantica, o se autorizzati dalla legge ad accertare, prevenire, indagare o perseguire reati.
3. I deployer di un sistema di riconoscimento delle emozioni o di un sistema di categorizzazione biometrica informano le persone fisiche che vi sono esposte in merito al funzionamento del sistema e trattano i dati personali in conformità dei regolamenti (UE) 2016/679 e (UE) 2018/1725 e della direttiva (UE) 2016/680, a seconda dei casi. Tale obbligo non si applica ai sistemi di IA utilizzati per la categorizzazione biometrica e il riconoscimento delle emozioni autorizzati dalla legge per accertare, prevenire o indagare reati, fatte salve le tutele adeguate per i diritti e le libertà dei terzi e conformemente al diritto dell'Unione.

4. I deployer di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un "deep fake" rendono noto che il contenuto è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati. Qualora il contenuto faccia parte di un'analoga opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera.

I deployer di un sistema di IA che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati o se il contenuto generato dall'IA è stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.

5. Le informazioni di cui ai paragrafi da 1 a 4 sono fornite alle persone fisiche interessate in maniera chiara e distinguibile al più tardi al momento della prima interazione o esposizione. Le informazioni devono essere conformi ai requisiti di accessibilità applicabili.
6. I paragrafi da 1 a 4 lasciano impregiudicati i requisiti e gli obblighi di cui al capo III, così come gli altri obblighi di trasparenza stabiliti dal diritto dell'Unione o nazionale per i deployer dei sistemi di IA.

7. L'ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei contenuti generati o manipolati artificialmente. La Commissione può adottare atti di esecuzione per approvare tali codici di buone pratiche secondo la procedura di cui all'articolo 56, paragrafo 6. Se ritiene che il codice non sia adeguato, la Commissione può adottare un atto di esecuzione che specifichi norme comuni per l'attuazione di tali obblighi secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Capo V

Modelli di ia per finalità generali

SEZIONE 1

REGOLE DI CLASSIFICAZIONE

Articolo 51

Classificazione dei modelli di IA per finalità generali come modelli di IA per finalità generali con rischio sistemico

1. Un modello di IA per finalità generali è classificato come modello di IA per finalità generali con rischio sistemico se soddisfa una delle condizioni seguenti:
- a) presenta capacità di impatto elevato valutate sulla base di strumenti tecnici e metodologie adeguati, compresi indicatori e parametri di riferimento;

- b) sulla base di una decisione della Commissione, *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici, presenta capacità o un impatto equivalenti a quelli di cui alla lettera a), tenendo conto dei criteri di cui all'allegato XIII.
2. Si presume che un modello di IA per finalità generali abbia capacità di impatto elevato a norma del paragrafo 1, lettera a), quando la quantità cumulativa di calcolo utilizzata per il suo addestramento misurata in operazioni in virgola mobile è superiore a 10^{25} .
3. La Commissione adotta atti delegati a norma dell'articolo 97 per modificare le soglie di cui ai paragrafi 1 e 2 del presente articolo, nonché per integrare parametri di riferimento e indicatori alla luce degli sviluppi tecnologici in evoluzione, quali miglioramenti algoritmici o una maggiore efficienza dell'hardware, ove necessario, affinché tali soglie riflettano lo stato dell'arte.

Articolo 52

Procedura

1. Se un modello di IA per finalità generali soddisfa la condizione di cui all'articolo 51, paragrafo 1, lettera a), il fornitore pertinente informa la Commissione senza ritardo e in ogni caso entro due settimane dal soddisfacimento di tale requisito o dal momento in cui viene a conoscenza che tale requisito sarà soddisfatto. Tale notifica comprende le informazioni necessarie a dimostrare che il requisito in questione è stato soddisfatto. Se la Commissione viene a conoscenza di un modello di IA per finalità generali che presenta rischi sistemici di cui non è stata informata, può decidere di designarlo come modello con rischio sistemico.

2. Il fornitore di un modello di IA per finalità generali che soddisfa la condizione di cui all'articolo 51, paragrafo 1, lettera a), può presentare, unitamente alla sua notifica, argomentazioni sufficientemente fondate per dimostrare che, in via eccezionale, sebbene soddisfi tale requisito, il modello di IA per finalità generali non presenta, a causa delle sue caratteristiche specifiche, rischi sistemici e non dovrebbe essere pertanto classificato come modello di IA per finalità generali con rischio sistemico.
3. Se la Commissione conclude che le argomentazioni presentate a norma del paragrafo 2 non sono sufficientemente fondate e il fornitore in questione non è stato in grado di dimostrare che il modello di IA per finalità generali non presenta, per le sue caratteristiche specifiche, rischi sistemici, essa respinge tali argomentazioni e il modello di IA per finalità generali è considerato un modello di IA per finalità generali con rischio sistemico.
4. La Commissione può designare un modello di IA per finalità generali come modello che presenta rischi sistemici, *ex officio* o a seguito di una segnalazione qualificata del gruppo di esperti scientifici a norma dell'articolo 90, paragrafo 1, lettera a), sulla base dei criteri di cui all'allegato XIII.

Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 97 per modificare l'allegato XIII specificando e aggiornando i criteri di cui a tale allegato.

5. Su richiesta motivata di un fornitore il cui modello è stato designato come modello di IA per finalità generali con rischio sistemico a norma del paragrafo 4, la Commissione, tenendo conto della richiesta, può decidere di valutare nuovamente se si possa ancora ritenere che il modello di IA per finalità generali presenti rischi sistemici sulla base dei criteri di cui all'allegato XIII. Tale richiesta contiene motivi oggettivi, dettagliati e nuovi emersi dopo la decisione di designazione. I fornitori possono chiedere una nuova valutazione non prima di sei mesi dopo la decisione di designazione. Se la Commissione, a seguito della nuova valutazione, decide di mantenere la designazione come modello di IA per finalità generali con rischio sistemico, i fornitori possono chiedere una nuova valutazione non prima di sei mesi dopo tale decisione.
6. La Commissione garantisce che sia pubblicato un elenco di modelli di IA per finalità generali con rischio sistemico e lo mantiene aggiornato, fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale.

SEZIONE 2

OBBLIGHI DEI FORNITORI DI MODELLI DI IA PER FINALITÀ GENERALI

Articolo 53

Obblighi dei fornitori di modelli di IA per finalità generali

1. I fornitori di modelli di IA per finalità generali:
 - a) redigono e mantengono aggiornata la documentazione tecnica del modello, compresi il processo di addestramento e prova e i risultati della sua valutazione, che contiene almeno le informazioni di cui all'allegato XI affinché possa essere trasmessa, su richiesta, all'ufficio per l'IA e alle autorità nazionali competenti;
 - b) elaborano, mantengono aggiornate e mettono a disposizione informazioni e documentazione per i fornitori di sistemi di IA che intendono integrare il modello di IA per finalità generali nei loro sistemi di IA. Fatta salva la necessità di rispettare e proteggere i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali conformemente al diritto dell'Unione e nazionale, le informazioni e la documentazione:
 - i) consentono ai fornitori di sistemi di IA di avere una buona comprensione delle capacità e dei limiti del modello di IA per finalità generali e di adempiere ai loro obblighi a norma del presente regolamento; nonché
 - ii) contengono almeno gli elementi di cui all'allegato XII;

- c) attuano una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e diritti ad esso collegati e, in particolare, a individuare e rispettare, anche attraverso tecnologie all'avanguardia, una riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790;
 - d) redigono e mettono a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali, secondo un modello fornito dall'ufficio per l'IA.
2. Gli obblighi di cui al paragrafo 1, lettere a) e b), non si applicano ai fornitori di modelli di IA rilasciati con licenza libera e open source che consentono l'accesso, l'uso, la modifica e la distribuzione del modello e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici. Tale eccezione non si applica ai modelli di IA per finalità generali con rischi sistemici.
3. I fornitori di modelli di IA per finalità generali collaborano, secondo necessità, con la Commissione e le autorità nazionali competenti nell'esercizio delle loro competenze e dei loro poteri a norma del presente regolamento.

4. I fornitori di modelli di IA per finalità generali possono basarsi su codici di buone pratiche ai sensi dell'articolo 56 per dimostrare la conformità agli obblighi di cui al paragrafo 1 del presente articolo, finché non è pubblicata una norma armonizzata. La conformità alle norme armonizzate europee garantisce ai fornitori la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi. I fornitori di modelli di IA per finalità generali che non aderiscono a un codice di buone pratiche approvato dimostrano mezzi alternativi adeguati di conformità ai fini di approvazione da parte della Commissione.
5. Allo scopo di agevolare la conformità all'allegato XI, in particolare al punto 2, lettere d) ed e), alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 97 per specificare le metodologie di misurazione e di calcolo al fine di consentire che la documentazione sia comparabile e verificabile.
6. Alla Commissione è conferito il potere di adottare atti delegati a norma dell'articolo 97, paragrafo 2, per modificare gli allegati XI e XII alla luce degli sviluppi tecnologici in evoluzione.
7. Le informazioni o la documentazione ottenute a norma del presente articolo, compresi i segreti commerciali, sono trattate in conformità degli obblighi di riservatezza di cui all'articolo 78.

Articolo 54

Rappresentanti autorizzati dei fornitori di modelli di IA per finalità generali

1. Prima di immettere sul mercato dell'Unione un modello di IA per finalità generali, i fornitori stabiliti in paesi terzi nominano, mediante mandato scritto, un rappresentante autorizzato stabilito nell'Unione.

2. Il fornitore consente al suo rappresentante autorizzato di eseguire i compiti specificati nel mandato ricevuto dal fornitore.
3. Il rappresentante autorizzato esegue i compiti specificati nel mandato ricevuto dal fornitore. Fornisce una copia del mandato all'ufficio per l'IA, su richiesta, in una delle lingue ufficiali delle istituzioni dell'Unione. Ai fini del presente regolamento, il mandato consente al rappresentante autorizzato di eseguire i compiti seguenti:
 - a) verificare che la documentazione tecnica di cui all'allegato XI sia stata redatta e che tutti gli obblighi di cui all'articolo 53 e, se del caso, all'articolo 55 siano stati adempiuti dal fornitore;
 - b) tenere a disposizione dell'ufficio per l'IA e delle autorità nazionali competenti una copia della documentazione tecnica di cui all'allegato XI per un periodo di 10 anni dalla data in cui il modello di IA per finalità generali è stato immesso sul mercato e i dati di contatto del fornitore che ha nominato il rappresentante autorizzato;
 - c) fornire all'ufficio per l'IA, su richiesta motivata, tutte le informazioni e la documentazione, comprese quelle di cui alla lettera b), necessarie per dimostrare la conformità agli obblighi di cui al presente capo;
 - d) cooperare con l'ufficio per l'IA e le autorità competenti, su richiesta motivata, in qualsiasi azione intrapresa da queste ultime in relazione al modello di IA per finalità generali, anche quando il modello è integrato nei sistemi di IA immessi sul mercato o messi in servizio nell'Unione.

4. Il mandato consente al rappresentante autorizzato di essere interlocutore, in aggiunta o in sostituzione del fornitore, nei confronti dell'ufficio per l'IA o delle autorità competenti per tutte le questioni relative al rispetto del presente regolamento.
5. Il rappresentante autorizzato pone fine al mandato se ritiene o ha motivi di ritenere che il fornitore agisca in contrasto con i propri obblighi a norma del presente regolamento. In tal caso, comunica immediatamente anche all'ufficio per l'IA la cessazione del mandato e i relativi motivi.
6. L'obbligo di cui al presente articolo non si applica ai fornitori di modelli di IA per finalità generali rilasciati con licenza libera e open source che consentono l'accesso, l'uso, la modifica e la distribuzione del modello e i cui parametri, compresi i pesi, le informazioni sull'architettura del modello e le informazioni sull'uso del modello, sono resi pubblici, tranne nel caso in cui i modelli di IA per finalità generali presentino rischi sistemici.

SEZIONE 3

OBBLIGHI DEI FORNITORI DI MODELLI DI IA PER FINALITÀ GENERALI CON RISCHIO SISTEMICO

Articolo 55

Obblighi dei fornitori di modelli di IA per finalità generali con rischio sistemico

1. In aggiunta agli obblighi di cui agli articoli 53 e 54, i fornitori di modelli di IA per finalità generali con rischio sistemico:
 - a) effettuano una valutazione dei modelli in conformità di protocolli e strumenti standardizzati che rispecchino lo stato dell'arte, anche svolgendo e documentando il test contraddittorio (adversarial testing) del modello al fine di individuare e attenuare i rischi sistemici;
 - b) valutano e attenuano i possibili rischi sistemici a livello dell'Unione, comprese le loro fonti, che possono derivare dallo sviluppo, dall'immissione sul mercato o dall'uso di modelli di IA per finalità generali con rischio sistemico;
 - c) tengono traccia, documentano e riferiscono senza indebito ritardo all'ufficio per l'IA e, se del caso, alle autorità nazionali competenti, le informazioni pertinenti su incidenti gravi ed eventuali misure correttive per porvi rimedio;
 - d) garantiscono un livello adeguato di protezione della cibersicurezza per quanto riguarda il modello di IA per finalità generali con rischio sistemico e l'infrastruttura fisica del modello.

2. I fornitori di modelli di IA per finalità generali con rischio sistemico possono basarsi su codici di buone pratiche ai sensi dell'articolo 56 per dimostrare la conformità agli obblighi di cui al paragrafo 1 del presente articolo, fino alla pubblicazione di una norma armonizzata. La conformità alle norme armonizzate europee garantisce ai fornitori la presunzione di conformità nella misura in cui tali norme contemplano tali obblighi. I fornitori di modelli di IA per finalità generali con rischi sistemici che non aderiscono a un codice di buone pratiche approvato o che non si conformano alle norme armonizzate europee devono dimostrare mezzi alternativi adeguati di conformità ai fini della valutazione da parte della Commissione.
3. Le informazioni o la documentazione ottenute a norma del presente articolo, compresi i segreti commerciali, sono trattate in conformità degli obblighi di riservatezza di cui all'articolo 78.

SEZIONE 4

CODICI DI BUONE PRATICHE

Articolo 56

Codici di buone pratiche

1. L'ufficio per l'IA incoraggia e agevola l'elaborazione di codici di buone pratiche a livello dell'Unione al fine di contribuire alla corretta applicazione del presente regolamento, tenendo conto degli approcci internazionali.

2. L'ufficio per l'IA e il consiglio per l'IA mirano a garantire che i codici di buone pratiche contemplino almeno gli obblighi di cui agli articoli 53 e 55, compreso quanto segue:
- a) i mezzi per garantire che le informazioni di cui all'articolo 53, paragrafo 1, lettere a) e b), siano mantenute aggiornate alla luce degli sviluppi tecnologici e di mercato;
 - b) un adeguato livello di dettaglio nella sintesi dei contenuti utilizzati per l'addestramento;
 - c) l'individuazione del tipo e della natura dei rischi sistemici a livello dell'Unione, comprese le rispettive fonti, se del caso;
 - d) le misure, le procedure e le modalità per la valutazione e la gestione dei rischi sistemici a livello dell'Unione, compresa la relativa documentazione, che devono essere proporzionate ai rischi e tenere conto della loro gravità e probabilità e delle sfide specifiche nell'affrontare tali rischi alla luce dei modi possibili in cui tali rischi possono emergere e concretizzarsi lungo la catena del valore dell'IA.
3. L'ufficio per l'IA può invitare tutti i fornitori di modelli di IA per finalità generali, nonché le pertinenti autorità nazionali competenti, a partecipare all'elaborazione dei codici di buone pratiche. Le organizzazioni della società civile, l'industria, il mondo accademico e altri pertinenti portatori di interessi, quali i fornitori a valle e gli esperti indipendenti, possono sostenere il processo.

4. L'ufficio per l'IA e il consiglio per l'IA mirano a garantire che i codici di buone pratiche definiscano chiaramente i loro obiettivi specifici e contengano impegni o misure, compresi, se del caso, indicatori chiave di prestazione, volti ad assicurare il conseguimento di tali obiettivi e che tengano debitamente conto delle esigenze e degli interessi di tutte le parti interessate, anche delle persone interessate, a livello dell'Unione.
5. L'ufficio per l'IA mira a garantire che i partecipanti all'elaborazione dei codici di buone pratiche riferiscano periodicamente all'ufficio per l'IA in merito all'attuazione degli impegni, alle misure adottate e ai loro esiti, anche rispetto agli indicatori chiave di prestazione, se del caso. Gli indicatori chiave di prestazione e gli impegni di comunicazione riflettono le differenze in termini di dimensioni e capacità tra i vari partecipanti.
6. L'ufficio per l'IA e il consiglio per l'IA monitorano e valutano periodicamente il conseguimento degli obiettivi dei codici di buone pratiche da parte dei partecipanti e il loro contributo alla corretta applicazione del presente regolamento. L'ufficio per l'IA e il consiglio per l'IA valutano se i codici di buone pratiche contemplano gli obblighi di cui agli articoli 53 e 55, 4e monitorano e valutano periodicamente il conseguimento dei loro obiettivi. Essi pubblicano la loro valutazione riguardante l'adeguatezza dei codici di buone pratiche.

La Commissione può approvare, mediante atto di esecuzione, un codice di buone pratiche e conferire ad esso una validità generale all'interno dell'Unione. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

7. L'ufficio per l'IA può invitare tutti i fornitori di modelli di IA per finalità generali ad aderire ai codici di buone pratiche. Per i fornitori di modelli di IA per finalità generali che non presentano rischi sistemici, tale adesione può essere limitata agli obblighi di cui all'articolo 53, a meno che essi dichiarino esplicitamente il loro interesse ad aderire al codice nella sua interezza.
8. L'ufficio per l'IA incoraggia e agevola, se del caso, anche il riesame e l'adeguamento dei codici di buone pratiche, in particolare alla luce di norme emergenti. L'ufficio per l'IA fornisce assistenza per quanto riguarda la valutazione delle norme disponibili.
9. I codici di buone pratiche sono pronti al più tardi entro ... [nove mesi dalla data di entrata in vigore del presente regolamento]. L'ufficio per l'IA adotta le misure necessarie, compreso l'invito ai fornitori di cui al paragrafo 7.

Qualora entro ... [12 mesi dalla data di entrata in vigore del presente regolamento], un codice di buone pratiche non possa essere portato a termine, o qualora l'ufficio per l'IA lo ritenga non adeguato a seguito della valutazione di cui al paragrafo 6 del presente articolo, la Commissione può prevedere, mediante atti di esecuzione, norme comuni per l'attuazione degli obblighi di cui agli articoli 53 e 55, comprese le questioni di cui al paragrafo 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Capo VI

Misure a sostegno dell'innovazione

Articolo 57

Spazi di sperimentazione normativa per l'IA

1. Gli Stati membri provvedono affinché le loro autorità competenti istituiscano almeno uno spazio di sperimentazione normativa per l'IA a livello nazionale, che sia operativo entro ... [24 mesi dalla data di entrata in vigore del presente regolamento]. Tale spazio di sperimentazione può essere inoltre istituito congiuntamente con le autorità competenti di altri Stati membri. La Commissione può fornire assistenza tecnica, consulenza e strumenti per l'istituzione e il funzionamento degli spazi di sperimentazione normativa per l'IA.

L'obbligo di cui al primo comma può essere soddisfatto anche partecipando a uno spazio di sperimentazione esistente nella misura in cui tale partecipazione fornisca un livello equivalente di copertura nazionale per gli Stati membri partecipanti.
2. Possono essere altresì istituiti ulteriori spazi di sperimentazione normativa per l'IA a livello regionale o locale, o congiuntamente con le autorità competenti di altri Stati membri.
3. Il Garante europeo della protezione dei dati può inoltre istituire uno spazio di sperimentazione normativa per l'IA per le istituzioni, gli organi e gli organismi dell'Unione e può esercitare i ruoli e i compiti delle autorità nazionali competenti conformemente al presente capo.

4. Gli Stati membri provvedono affinché le autorità competenti di cui ai paragrafi 1 e 2 assegnino risorse sufficienti per conformarsi al presente articolo in maniera efficace e tempestiva. Se del caso, le autorità nazionali competenti cooperano con altre autorità pertinenti e possono consentire il coinvolgimento di altri attori all'interno dell'ecosistema dell'IA. Il presente articolo lascia impregiudicati gli altri spazi di sperimentazione normativa istituiti a norma del diritto dell'Unione o nazionale. Gli Stati membri garantiscono un livello adeguato di cooperazione tra le autorità che controllano tali altri spazi di sperimentazione e le autorità nazionali competenti.
5. Gli spazi di sperimentazione normativa per l'IA istituiti a norma del paragrafo 1 garantiscono un ambiente controllato che promuove l'innovazione e facilita lo sviluppo, l'addestramento, la sperimentazione e la convalida di sistemi di IA innovativi per un periodo di tempo limitato prima della loro immissione sul mercato o della loro messa in servizio conformemente a un piano specifico dello spazio di sperimentazione concordato tra i fornitori o i potenziali fornitori e l'autorità competente. Tali spazi di sperimentazione possono comprendere prove in condizioni reali soggette a controllo nei medesimi spazi.
6. Le autorità competenti, se del caso, forniscono orientamenti e garantiscono il controllo e il sostegno nell'ambito dello spazio di sperimentazione normativa per l'IA al fine di individuare i rischi, in particolare per quanto riguarda i diritti fondamentali, la salute e la sicurezza, le prove, le misure di attenuazione e la loro efficacia, in relazione agli obblighi e ai requisiti del presente regolamento e, se del caso, di altre disposizioni del diritto dell'Unione e nazionale, la conformità ai quali è soggetta a controllo nell'ambito dello spazio di sperimentazione.
7. Le autorità competenti forniscono ai fornitori e ai potenziali fornitori che partecipano allo spazio di sperimentazione normativa per l'IA orientamenti sulle aspettative normative e sulle modalità per soddisfare i requisiti e gli obblighi di cui al presente regolamento.

Su richiesta del fornitore o del potenziale fornitore del sistema di IA, l'autorità competente fornisce una prova scritta delle attività svolte con successo nello spazio di sperimentazione. L'autorità competente fornisce inoltre una relazione di uscita che illustra in dettaglio le attività svolte nello spazio di sperimentazione e i relativi risultati e le conclusioni dell'apprendimento. I fornitori possono utilizzare tale documentazione per dimostrare la loro conformità al presente regolamento attraverso la procedura di valutazione della conformità o le pertinenti attività di vigilanza del mercato. A tale riguardo, la relazione di uscita e la prova scritta fornite dall'autorità nazionale competente sono prese favorevolmente in considerazione dalle autorità di vigilanza del mercato e dagli organismi notificati, al fine di accelerare le procedure di valutazione della conformità in misura ragionevole.

8. Fatte salve le disposizioni in materia di riservatezza di cui all'articolo 78, e con l'accordo del fornitore o del potenziale fornitore, la Commissione e il consiglio per l'IA sono autorizzati ad accedere alle relazioni di uscita e ne tengono conto, se del caso, nell'esercizio dei loro compiti a norma del presente regolamento. Se sia il fornitore o il potenziale fornitore sia l'autorità nazionale competente acconsentono esplicitamente, la relazione di uscita può essere messa a disposizione del pubblico attraverso la piattaforma unica di informazione di cui al presente articolo.
9. L'istituzione di spazi di sperimentazione normativa per l'IA mira a contribuire agli obiettivi seguenti:
 - a) migliorare la certezza del diritto al fine di conseguire la conformità normativa al presente regolamento o, se del caso, ad altre applicabili disposizioni di diritto dell'Unione e nazionale;
 - b) sostenere la condivisione delle migliori pratiche attraverso la cooperazione con le autorità coinvolte nello spazio di sperimentazione normativa per l'IA;

- c) promuovere l'innovazione e la competitività e agevolare lo sviluppo di un ecosistema di IA;
 - d) contribuire all'apprendimento normativo basato su dati concreti;
 - e) agevolare e accelerare l'accesso al mercato dell'Unione per i sistemi di IA, in particolare se forniti dalle PMI, comprese le start-up.
10. Le autorità nazionali competenti garantiscono che, nella misura in cui i sistemi di IA innovativi comportano il trattamento di dati personali o rientrano altrimenti nell'ambito di competenza di altre autorità nazionali o autorità competenti che forniscono o sostengono l'accesso ai dati, le autorità nazionali per la protezione dei dati e tali altre autorità nazionali o competenti siano associate al funzionamento dello spazio di sperimentazione normativa per l'IA e partecipino al controllo di tali aspetti nei limiti dei rispettivi compiti e poteri.
11. Gli spazi di sperimentazione normativa per l'IA non pregiudicano i poteri correttivi o di controllo delle autorità competenti che controllano gli spazi di sperimentazione, anche a livello regionale o locale. Qualsiasi rischio significativo per la salute e la sicurezza e i diritti fondamentali individuato durante lo sviluppo e le prove di tali sistemi di IA comporta adeguate misure di attenuazione. Le autorità nazionali competenti hanno il potere di sospendere, in via temporanea o permanente, il processo di prova o la partecipazione allo spazio di sperimentazione, se non è possibile un'attenuazione efficace, e informano l'ufficio per l'IA di tale decisione. Le autorità nazionali competenti esercitano i loro poteri di controllo entro i limiti del pertinente diritto, utilizzando i loro poteri discrezionali nell'attuazione delle disposizioni giuridiche per quanto riguarda uno specifico progetto di spazio di sperimentazione normativa per l'IA, con l'obiettivo di promuovere l'innovazione nell'IA nell'Unione.

12. I fornitori e i potenziali fornitori partecipanti allo spazio di sperimentazione normativa per l'IA restano responsabili ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni arrecati a terzi a seguito della sperimentazione che ha luogo nello spazio di sperimentazione. Tuttavia, a condizione che i potenziali fornitori rispettino il piano specifico e i termini e le condizioni di partecipazione e seguano in buona fede gli orientamenti forniti dall'autorità nazionale competente, quest'ultima non infligge alcuna sanzione amministrativa in caso di violazione del presente regolamento. Qualora altre autorità competenti responsabili del diritto dell'Unione e nazionale abbiano partecipato attivamente al controllo del sistema di IA nello spazio di sperimentazione e abbiano fornito orientamenti ai fini della conformità, nessuna sanzione amministrativa pecuniaria è inflitta in relazione a tali disposizioni di diritto.
13. Gli spazi di sperimentazione normativa per l'IA sono progettati e attuati in modo tale da agevolare, se del caso, la cooperazione transfrontaliera tra le autorità nazionali competenti.
14. Le autorità nazionali competenti coordinano le loro attività e cooperano nel quadro del consiglio per l'IA.
15. Le autorità nazionali competenti informano l'ufficio per l'IA e il consiglio per l'IA di uno spazio di sperimentazione e possono chiedere sostegno e orientamenti. L'ufficio per l'IA mette a disposizione del pubblico l'elenco degli spazi di sperimentazione normativa pianificati ed esistenti e lo mantiene aggiornato al fine di incoraggiare una maggiore interazione negli spazi di sperimentazione e nella cooperazione transfrontaliera.

16. Le autorità nazionali competenti presentano relazioni annuali all'ufficio per l'IA e al consiglio per l'IA a decorrere dall'anno successivo all'istituzione dello spazio di sperimentazione normativa per l'IA e successivamente ogni anno fino alla sua cessazione, nonché una relazione definitiva. Tali relazioni contengono informazioni sui progressi e sui risultati dell'attuazione di tali spazi di sperimentazione, comprese le migliori pratiche, gli incidenti, gli insegnamenti tratti e le raccomandazioni sulla loro configurazione e, ove pertinente, sull'applicazione ed eventuale revisione del presente regolamento, inclusi i rispettivi atti delegati e di esecuzione, e sull'applicazione di altre disposizioni di diritto dell'Unione soggette a controllo da parte delle autorità competenti nell'ambito dello spazio di sperimentazione. Le autorità nazionali competenti mettono tali relazioni annuali o estratti delle stesse a disposizione del pubblico online. La Commissione tiene conto, se del caso, delle relazioni annuali nell'esercizio dei suoi compiti a norma del presente regolamento.
17. La Commissione sviluppa un'interfaccia unica e dedicata contenente tutte le informazioni pertinenti relative agli spazi di sperimentazione normativa per l'IA per permettere ai portatori di interessi di interagire con gli spazi di sperimentazione normativa per l'IA e di formulare richieste di informazioni presso le autorità competenti e di chiedere orientamenti non vincolanti sulla conformità di prodotti, servizi e modelli aziendali innovativi che integrano le tecnologie di IA, a norma dell'articolo 62, paragrafo 1, lettera c). La Commissione si coordina proattivamente con le autorità nazionali competenti, se del caso.

Articolo 58

Modalità dettagliate e funzionamento degli spazi di sperimentazione normativa per l'IA

1. Onde evitare la frammentazione nell'intera Unione, la Commissione adotta atti di esecuzione che precisano le modalità dettagliate per l'istituzione, lo sviluppo, l'attuazione, il funzionamento e la supervisione degli spazi di sperimentazione normativa per l'IA. Tali atti di esecuzione comprendono principi comuni sulle questioni seguenti:
 - a) criteri di ammissibilità e selezione per la partecipazione allo spazio di sperimentazione normativa per l'IA;
 - b) procedure per la domanda, la partecipazione, il monitoraggio, l'uscita dallo spazio di sperimentazione normativa per l'IA e la sua cessazione, compresi il piano dello spazio di sperimentazione e la relazione di uscita;
 - c) i termini e le condizioni applicabili ai partecipanti.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

2. Gli atti di esecuzione di cui al paragrafo 1 garantiscono:
 - a) che gli spazi di sperimentazione normativa per l'IA siano aperti a qualsiasi fornitore o potenziale fornitore richiedente di un sistema di IA che soddisfi criteri di ammissibilità e selezione trasparenti ed equi, e che le autorità nazionali competenti informino i richiedenti della loro decisione entro tre mesi dalla domanda;

- b) che gli spazi di sperimentazione normativa consentano un accesso ampio e paritario e tengano il passo con la domanda di partecipazione; i fornitori e i potenziali fornitori possono anche presentare domande in partenariato con gli deployers e con altri terzi interessati;
- c) che le modalità dettagliate e le condizioni relative agli spazi di sperimentazione normativa per l'IA sostengano la flessibilità, nella massima misura possibile, affinché le autorità nazionali competenti istituiscano e gestiscano i loro spazi di sperimentazione normativa per l'IA;
- d) che l'accesso agli spazi di sperimentazione normativa per l'IA sia gratuito per le PMI, comprese le start-up, fatti salvi i costi straordinari che le autorità nazionali competenti possono recuperare in maniera equa e proporzionata;
- e) che i fornitori e i potenziali fornitori siano agevolati, attraverso i risultati dell'apprendimento degli spazi di sperimentazione normativa per l'IA, a conformarsi agli obblighi di valutazione della conformità di cui al presente regolamento e all'applicazione volontaria dei codici di condotta di cui all'articolo 95;
- f) che gli spazi di sperimentazione normativa per l'IA facilitino il coinvolgimento di altri attori pertinenti nell'ambito dell'ecosistema dell'IA, quali organismi notificati e organizzazioni di normazione, PMI, comprese start-up, imprese, innovatori, impianti di prova e sperimentazione, laboratori di ricerca e sperimentazione e poli europei dell'innovazione digitale, centri di eccellenza e singoli ricercatori, al fine di consentire e facilitare la cooperazione con i settori pubblico e privato;

- g) che le procedure, i processi e i requisiti amministrativi per l'applicazione, la selezione, la partecipazione e l'uscita dallo spazio di sperimentazione normativa per l'IA siano semplici, facilmente intelligibili, comunicati chiaramente per agevolare la partecipazione delle PMI, comprese le start-up, con capacità giuridiche e amministrative limitate e siano razionalizzati in tutta l'Unione, al fine di evitare la frammentazione e che la partecipazione a uno spazio di sperimentazione normativa per l'IA istituito da uno Stato membro o dal Garante europeo della protezione dei dati sia reciprocamente e uniformemente riconosciuta e produca gli stessi effetti giuridici nell'intera Unione;
 - h) che la partecipazione allo spazio di sperimentazione normativa per l'IA sia limitata a un periodo adeguato alla complessità e alla portata del progetto, che può essere prorogato dall'autorità nazionale competente;
 - i) che gli spazi di sperimentazione normativa per l'IA agevolino lo sviluppo di strumenti e infrastrutture per la sperimentazione, l'analisi comparativa, la valutazione e la spiegazione delle dimensioni dei sistemi di IA pertinenti per l'apprendimento normativo, quali l'accuratezza, la robustezza e la cibersicurezza, nonché le misure per attenuare i rischi per i diritti fondamentali e la società in generale.
3. I potenziali fornitori degli spazi di sperimentazione normativa per l'IA, soprattutto le PMI e le start-up, sono indirizzati, se del caso, a servizi di pre-diffusione, quali gli orientamenti sull'attuazione del presente regolamento, ad altri servizi a valore aggiunto, quali l'assistenza per i documenti di normazione e la certificazione, gli impianti di prova e sperimentazione, i poli europei dell'innovazione digitale e i centri di eccellenza.

4. Quando valutano la possibilità di autorizzare prove in condizioni reali sottoposte a controllo nel quadro di uno spazio di sperimentazione normativa per l'IA da istituire a norma del presente articolo, le autorità nazionali competenti concordano in modo specifico con i partecipanti i termini e le condizioni di tali prove e, in particolare, le tutele adeguate al fine di proteggere i diritti fondamentali, la salute e la sicurezza. Se del caso, cooperano con altre autorità nazionali competenti al fine di garantire pratiche coerenti in tutta l'Unione.

Articolo 59

Ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico

1. Nello spazio di sperimentazione normativa per l'IA, i dati personali legalmente raccolti per altre finalità possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione quando sono soddisfatte tutte le condizioni seguenti:
- a) i sistemi di IA sono sviluppati per salvaguardare un interesse pubblico rilevante da parte di un'autorità pubblica o di un'altra persona fisica o giuridica e in uno o più dei settori seguenti:
 - i) la sicurezza pubblica e la sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari;
 - ii) un elevato livello di protezione e di miglioramento della qualità dell'ambiente, la tutela della biodiversità, la protezione contro l'inquinamento, le misure per la transizione verde, la mitigazione dei cambiamenti climatici e l'adattamento ad essi;

- iii) la sostenibilità energetica;
 - iv) la sicurezza e la resilienza dei sistemi di trasporto e della mobilità, delle infrastrutture critiche e delle reti;
 - v) l'efficienza e la qualità della pubblica amministrazione e dei servizi pubblici;
- b) i dati trattati sono necessari per il rispetto di uno o più dei requisiti di cui al capo III, sezione 2, qualora tali requisiti non possano essere efficacemente soddisfatti mediante il trattamento di dati anonimizzati, sintetici o di altri dati non personali;
- c) esistono meccanismi di monitoraggio efficaci per individuare eventuali rischi elevati per i diritti e le libertà degli interessati di cui all'articolo 35 del regolamento (UE) 2016/679 e all'articolo 39 del regolamento (UE) 2018/1725 durante la sperimentazione nello spazio di sperimentazione e meccanismi di risposta per attenuare rapidamente tali rischi e, ove necessario, interrompere il trattamento;
- d) i dati personali da trattare nel contesto dello spazio di sperimentazione sono in un ambiente di trattamento dei dati funzionalmente separato, isolato e protetto sotto il controllo del potenziale fornitore e solo le persone autorizzate hanno accesso a tali dati;
- e) i fornitori possono condividere ulteriormente i dati originariamente raccolti solo in conformità del diritto dell'Unione in materia di protezione dei dati; i dati personali creati nello spazio di sperimentazione non possono essere condivisi al di fuori dello spazio di sperimentazione;

- f) il trattamento di dati personali nel contesto dello spazio di sperimentazione non comporta misure o decisioni aventi ripercussioni sugli interessati né incide sull'applicazione dei loro diritti sanciti dal diritto dell'Unione in materia di protezione dei dati personali;
- g) i dati personali trattati nell'ambito dello spazio di sperimentazione sono protetti mediante adeguate misure tecniche e organizzative e cancellati una volta terminata la partecipazione allo spazio di sperimentazione o al raggiungimento del termine del periodo di conservazione dei dati personali;
- h) i log del trattamento dei dati personali nel contesto dello spazio di sperimentazione sono conservati per la durata della partecipazione allo spazio di sperimentazione, salvo diversa disposizione del diritto dell'Unione o nazionale;
- i) una descrizione completa e dettagliata del processo e della logica alla base dell'addestramento, delle prove e della convalida del sistema di IA è conservata insieme ai risultati delle prove nell'ambito della documentazione tecnica di cui all'allegato IV;
- j) una breve sintesi del progetto di IA sviluppato nello spazio di sperimentazione, dei suoi obiettivi e dei risultati attesi è pubblicata sul sito web delle autorità competenti; tale obbligo non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo.

2. A fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro le minacce alla sicurezza pubblica e la prevenzione delle stesse, sotto il controllo e la responsabilità delle autorità di contrasto, il trattamento dei dati personali negli spazi di sperimentazione normativa per l'IA si basa su una specifica disposizione di diritto nazionale o dell'Unione ed è soggetto alle stesse condizioni cumulative di cui al paragrafo 1.
3. Il paragrafo 1 lascia impregiudicate le disposizioni del diritto dell'Unione o nazionale che escludono il trattamento dei dati personali per fini diversi da quelli espressamente menzionati in tali disposizioni, nonché il diritto dell'Unione o nazionale che stabilisce la base per il trattamento dei dati personali necessario ai fini dello sviluppo, delle prove e dell'addestramento di sistemi di IA innovativi o qualsiasi altra base giuridica, conformemente al diritto dell'Unione in materia di protezione dei dati personali.

Articolo 60

Prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

1. Le prove di sistemi di IA ad alto rischio in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA possono essere effettuate da fornitori o potenziali fornitori di sistemi di IA ad alto rischio elencati nell'allegato III, conformemente al presente articolo e al piano di prova in condizioni reali di cui al presente articolo, fatti salvi i divieti di cui all'articolo 5.

La Commissione, per mezzo di atti di esecuzione, specifica nel dettaglio gli elementi del piano di prova in condizioni reali. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Il presente paragrafo lascia impregiudicato il diritto dell'Unione o nazionale concernente le prove in condizioni reali di sistemi di IA ad alto rischio relativi a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I.

2. I fornitori o potenziali fornitori possono effettuare prove dei sistemi di IA ad alto rischio di cui all'allegato III in condizioni reali in qualsiasi momento prima dell'immissione sul mercato o della messa in servizio del sistema di IA, da soli o in partenariato con uno o più deployer o potenziali deployer.
3. Le prove di sistemi di IA ad alto rischio in condizioni reali a norma del presente articolo non pregiudicano alcun esame etico che sia richiesto dal diritto dell'Unione o nazionale.
4. I fornitori o potenziali fornitori possono effettuare le prove in condizioni reali solo se sono soddisfatte tutte le condizioni seguenti:
 - a) il fornitore o potenziale fornitore ha elaborato un piano di prova in condizioni reali e lo ha presentato all'autorità di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali;
 - b) l'autorità nazionale di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali ha approvato le prove in condizioni reali e il piano di prova in condizioni reali; se l'autorità di vigilanza del mercato non ha fornito una risposta entro 30 giorni, le prove in condizioni reali e il piano di prova in condizioni reali sono da intendersi approvati; se il diritto nazionale non prevede un'approvazione tacita, le prove in condizioni reali restano soggette ad autorizzazione;

- c) il fornitore o potenziale fornitore, ad eccezione dei fornitori o dei potenziali fornitori dei sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori delle attività di contrasto, della migrazione, dell'asilo e della gestione del controllo delle frontiere, e dei sistemi di IA ad alto rischio di cui all'allegato III, punto 2, ha registrato la prova in condizioni reali conformemente all'articolo 71, paragrafo 4, con un numero di identificazione unico a livello dell'Unione e con le informazioni di cui all'allegato IX; il fornitore o il potenziale fornitore di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 e 7, nei settori dell'attività di contrasto, della migrazione, dell'asilo e della gestione del controllo di frontiera, ha registrato la prova in condizioni reali in una sezione sicura non pubblica della banca dati UE ai sensi dell'articolo 49, paragrafo 4, lettera d), con un numero di identificazione unico a livello dell'Unione e con le informazioni ivi specificate; il fornitore o il potenziale fornitore di sistemi di IA ad alto rischio di cui all'allegato III, punto 2, ha registrato la prova in condizioni reali conformemente all'articolo 49, paragrafo 5;
- d) il fornitore o potenziale fornitore che effettua le prove in condizioni reali è stabilito nell'Unione o ha nominato un rappresentante legale che è stabilito nell'Unione;
- e) i dati raccolti e trattati ai fini delle prove in condizioni reali sono trasferiti a paesi terzi solo a condizione che siano poste in essere tutele adeguate e applicabili ai sensi del diritto dell'Unione;

- f) le prove in condizioni reali non durano più di quanto necessario per conseguire i rispettivi obiettivi e, in ogni caso, non più di sei mesi, che possono essere prorogati per un ulteriore periodo di sei mesi, previa notifica da parte del fornitore o del potenziale fornitore all'autorità di vigilanza del mercato, corredata della motivazione relativa alla necessità di tale proroga;
- g) i soggetti delle prove in condizioni reali che sono persone appartenenti a gruppi vulnerabili a causa della loro età o disabilità sono adeguatamente protetti;
- h) qualora un fornitore o potenziale fornitore organizzi le prove in condizioni reali in cooperazione con uno o più deployer o potenziali deployer, questi ultimi sono stati informati di tutti gli aspetti delle prove pertinenti per la loro decisione di partecipare e hanno ricevuto le istruzioni pertinenti per l'uso del sistema di IA di cui all'articolo 13; il fornitore o potenziale fornitore e il deployer o potenziale deployer concludono un accordo che ne specifica i ruoli e le responsabilità al fine di garantire la conformità alle disposizioni relative alle prove in condizioni reali ai sensi del presente regolamento e di altre disposizioni applicabili di diritto dell'Unione e nazionale;
- i) i soggetti delle prove in condizioni reali hanno dato il proprio consenso informato a norma dell'articolo 61 o, nel caso delle attività di contrasto, qualora la richiesta di consenso informato impedisca di sottoporre a prova il sistema di IA, le prove stesse e i risultati delle prove in condizioni reali non hanno alcun effetto negativo sui soggetti e i loro dati personali sono cancellati dopo lo svolgimento della prova;

- j) le prove in condizioni reali sono efficacemente supervisionate dal fornitore o potenziale fornitore, nonché dai deployer o dai potenziali deployer, tramite persone adeguatamente qualificate nel settore pertinente e dotate delle capacità, della formazione e dell'autorità necessarie per svolgere i loro compiti;
 - k) le previsioni, le raccomandazioni o le decisioni del sistema di IA possono essere efficacemente ribaltate e ignorate.
5. Qualsiasi soggetto delle prove in condizioni reali, o il suo rappresentante legale designato, a seconda dei casi, può, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione, ritirarsi dalle prove in qualsiasi momento revocando il proprio consenso informato e può chiedere la cancellazione immediata e permanente dei propri dati personali. La revoca del consenso informato non pregiudica le attività già svolte.
6. A norma dell'articolo 75, gli Stati membri conferiscono alle loro autorità di vigilanza del mercato il potere di imporre ai fornitori e ai potenziali fornitori di fornire informazioni, di effettuare ispezioni a distanza o in loco senza preavviso e di svolgere controlli sulla conduzione delle prove in condizioni reali e sui relativi sistemi di IA ad alto rischio. Le autorità di vigilanza del mercato si avvalgono di tali poteri per garantire lo sviluppo in sicurezza delle prove in condizioni reali.

7. Qualsiasi incidente grave individuato nel corso delle prove in condizioni reali è segnalato all'autorità nazionale di vigilanza del mercato conformemente all'articolo 73. Il fornitore o potenziale fornitore adotta misure di attenuazione immediate o, in mancanza di ciò, sospende le prove in condizioni reali fino a quando tale attenuazione non abbia luogo oppure vi pone fine. Il fornitore o potenziale fornitore stabilisce una procedura per il tempestivo ritiro del sistema di IA in seguito a tale cessazione delle prove in condizioni reali.
8. I fornitori o potenziali fornitori notificano all'autorità nazionale di vigilanza del mercato dello Stato membro in cui devono essere effettuate le prove in condizioni reali la sospensione o la cessazione delle prove in condizioni reali nonché i risultati finali.
9. Il fornitore o potenziale fornitore è responsabile ai sensi del diritto dell'Unione e nazionale applicabile in materia di responsabilità per eventuali danni causati nel corso delle prove in condizioni reali.

Articolo 61

Consenso informato a partecipare a prove in condizioni reali al di fuori degli spazi di sperimentazione normativa per l'IA

1. Ai fini delle prove in condizioni reali a norma dell'articolo 60, il consenso informato dato liberamente dai soggetti delle prove è ottenuto prima della loro partecipazione a tali prove e dopo che sono stati debitamente informati con indicazioni concise, chiare, pertinenti e comprensibili riguardanti:
 - a) la natura e gli obiettivi delle prove in condizioni reali e i possibili disagi che possono essere connessi alla loro partecipazione;
 - b) le condizioni alle quali devono essere effettuate le prove in condizioni reali, compresa la durata prevista della partecipazione del soggetto o dei soggetti;
 - c) i loro diritti e le garanzie riconosciute al soggetto in relazione alla loro partecipazione, in particolare il loro diritto di rifiutarsi di partecipare e il diritto di ritirarsi dalle prove in condizioni reali in qualsiasi momento, senza alcun conseguente pregiudizio e senza dover fornire alcuna giustificazione;
 - d) le modalità per richiedere che le previsioni, raccomandazioni o decisioni del sistema di IA siano ignorate o ribaltate;
 - e) il numero di identificazione unico a livello dell'Unione delle prove in condizioni reali conformemente all'articolo 60, paragrafo 4, lettera c), e i dati di contatto del fornitore o del suo rappresentante legale da cui è possibile ottenere ulteriori informazioni.

2. Il consenso informato è datato e documentato e una copia è consegnata ai soggetti delle prove o al loro rappresentante legale.

Articolo 62

Misure per i fornitori e i deployer, in particolare le PMI, comprese le start-up

1. Gli Stati membri intraprendono le azioni seguenti:
 - a) fornire alle PMI, comprese le start-up, con sede legale o una filiale nell'Unione, un accesso prioritario agli spazi di sperimentazione normativa per l'IA nella misura in cui soddisfano le condizioni di ammissibilità e i criteri di selezione; l'accesso prioritario non impedisce ad altre PMI, comprese le start-up, diverse da quelle di cui al presente paragrafo di accedere allo spazio di sperimentazione normativa per l'IA, purché soddisfino anche le condizioni di ammissibilità e i criteri di selezione;
 - b) organizzare specifiche attività di sensibilizzazione e formazione sull'applicazione del presente regolamento adattate alle esigenze delle PMI, comprese le start-up, dei deployers e, se del caso, delle autorità pubbliche locali;
 - c) utilizzare i canali dedicati esistenti e, ove opportuno, istituirne di nuovi per la comunicazione con le PMI, comprese le start-up, i deployers, altri innovatori e, se del caso, le autorità pubbliche locali, al fine di fornire consulenza e rispondere alle domande sull'attuazione del presente regolamento, anche per quanto riguarda la partecipazione agli spazi di sperimentazione normativa per l'IA;

- d) agevolare la partecipazione delle PMI e di altri portatori di interessi pertinenti al processo di sviluppo della normazione.
2. Nel fissare le tariffe per la valutazione della conformità a norma dell'articolo 43 si tiene conto degli interessi e delle esigenze specifici delle PMI fornitrici, comprese le start-up, riducendo tali tariffe proporzionalmente alle loro dimensioni, alle dimensioni del loro mercato e ad altri indicatori pertinenti.
3. L'ufficio per l'IA intraprende le azioni seguenti:
- a) fornire modelli standardizzati per i settori contemplati dal presente regolamento, come specificato dal consiglio per l'IA nella sua richiesta;
 - b) sviluppare e mantenere una piattaforma unica di informazione che fornisce informazioni di facile uso in relazione al presente regolamento per tutti gli operatori in tutta l'Unione;
 - c) organizzare adeguate campagne di comunicazione per sensibilizzare in merito agli obblighi derivanti dal presente regolamento;
 - d) valutare e promuovere la convergenza delle migliori pratiche nelle procedure di appalto pubblico in relazione ai sistemi di IA.

Articolo 63

Deroghe per operatori specifici

1. Le microimprese ai sensi della raccomandazione 2003/361/CE possono conformarsi a determinati elementi del sistema di gestione della qualità di cui all'articolo 17 del presente regolamento in modo semplificato, purché non abbiano imprese associate o collegate ai sensi di tale raccomandazione. A tal fine, la Commissione elabora orientamenti sugli elementi del sistema di gestione della qualità che possono essere rispettati in modo semplificato tenendo conto delle esigenze delle microimprese, senza incidere sul livello di protezione o sulla necessità di conformità ai requisiti per quanto riguarda i sistemi di IA ad alto rischio.
2. Il paragrafo 1 del presente articolo non è interpretato nel senso che esenta tali operatori dal rispetto di altri requisiti e obblighi di cui al presente regolamento, compresi quelli stabiliti agli articoli 9, 10, 11, 12, 13, 14, 15, 72 e 73.

Capo VII

Governance

SEZIONE 1

GOVERNANCE A LIVELLO DELL'UNIONE

Articolo 64

Ufficio per l'IA

1. La Commissione sviluppa le competenze e le capacità dell'Unione nel settore dell'IA attraverso l'ufficio per l'IA.
2. Gli Stati membri agevolano i compiti affidati all'ufficio per l'IA, come indicato nel presente regolamento.

Articolo 65

Istituzione e struttura del consiglio europeo per l'intelligenza artificiale

1. È istituito un consiglio europeo per l'intelligenza artificiale ("consiglio per l'IA").

2. Il consiglio per l'IA è composto di un rappresentante per Stato membro. Il Garante europeo della protezione dei dati partecipa come osservatore. Anche l'ufficio per l'IA partecipa alle riunioni del consiglio per l'IA senza partecipare alle votazioni. Altre autorità, organismi o esperti nazionali e dell'Unione possono essere invitati alle riunioni dal consiglio per l'IA caso per caso, qualora le questioni discusse siano di loro pertinenza.
3. Ciascun rappresentante è designato dal rispettivo Stato membro per un periodo di tre anni, rinnovabile una volta.
4. Gli Stati membri provvedono affinché i loro rappresentanti nel consiglio per l'IA:
 - a) dispongano delle competenze e dei poteri pertinenti nel proprio Stato membro in modo da contribuire attivamente allo svolgimento dei compiti del consiglio per l'IA di cui all'articolo 66;
 - b) siano designati come punto di contatto unico nei confronti del consiglio per l'IA e, se del caso tenendo conto delle esigenze degli Stati membri, come punto di contatto unico per i portatori di interessi;
 - c) abbiano il potere di agevolare la coerenza e il coordinamento tra le autorità nazionali competenti nel rispettivo Stato membro per quanto riguarda l'attuazione del presente regolamento, anche attraverso la raccolta di dati e informazioni pertinenti ai fini dello svolgimento dei loro compiti in seno al consiglio per l'IA.
5. I rappresentanti designati degli Stati membri adottano il regolamento interno del consiglio per l'IA a maggioranza di due terzi. Il regolamento interno stabilisce, in particolare, le procedure per il processo di selezione, la durata del mandato e le specifiche riguardanti i compiti del presidente, le modalità dettagliate relative al voto e l'organizzazione delle attività del consiglio per l'IA e dei suoi sottogruppi.

6. Il consiglio per l'IA istituisce due sottogruppi permanenti al fine di fornire una piattaforma di cooperazione e scambio tra le autorità di vigilanza del mercato e notificare le autorità su questioni relative rispettivamente alla vigilanza del mercato e agli organismi notificati.

Il sottogruppo permanente per la vigilanza del mercato dovrebbe fungere da gruppo di cooperazione amministrativa (ADCO) per il presente regolamento ai sensi dell'articolo 30 del regolamento (UE) 2019/1020.

Il consiglio per l'IA può istituire altri sottogruppi permanenti o temporanei, se del caso, ai fini dell'esame di questioni specifiche. Se del caso, i rappresentanti del forum consultivo di cui all'articolo 67 possono essere invitati a tali sottogruppi o a riunioni specifiche di tali sottogruppi in qualità di osservatori.

7. Il consiglio per l'IA è organizzato e gestito in modo che sia salvaguardata l'obiettività e l'imparzialità delle sue attività.
8. Il consiglio per l'IA è presieduto da uno dei rappresentanti degli Stati membri. L'ufficio per l'IA provvede alle funzioni di segretariato per il consiglio per l'IA, convoca le riunioni su richiesta della presidenza e prepara l'ordine del giorno in conformità dei compiti del consiglio per l'IA a norma del presente regolamento e del relativo regolamento interno.

Articolo 66
Compiti del consiglio per l'IA

Il consiglio per l'IA fornisce consulenza e assistenza alla Commissione e agli Stati membri al fine di agevolare l'applicazione coerente ed efficace del presente regolamento. A tal fine il consiglio per l'IA può in particolare:

- a) contribuire al coordinamento tra le autorità nazionali competenti responsabili dell'applicazione del presente regolamento e, in cooperazione con le autorità di vigilanza del mercato interessate e previo accordo di queste ultime, sostenere le attività congiunte delle autorità di vigilanza del mercato di cui all'articolo 74, paragrafo 11;
- b) raccogliere e condividere tra gli Stati membri conoscenze e migliori pratiche tecniche e normative;
- c) fornire consulenza sull'attuazione del presente regolamento, in particolare per quanto riguarda l'applicazione delle norme sui modelli di IA per finalità generali;
- d) contribuire all'armonizzazione delle pratiche amministrative negli Stati membri, anche in relazione alla deroga alle procedure di valutazione della conformità di cui all'articolo 46, al funzionamento degli spazi di sperimentazione normativa per l'IA e alle prove in condizioni reali di cui agli articoli 57, 59 e 60;

- e) su richiesta della Commissione o di propria iniziativa, formulare raccomandazioni e pareri scritti su qualsiasi questione pertinente relativa all'attuazione del presente regolamento e alla sua applicazione coerente ed efficace, tra l'altro:
- i) sull'elaborazione e l'applicazione di codici di condotta e codici di buone pratiche a norma del presente regolamento, nonché degli orientamenti della Commissione;
 - ii) sulla valutazione e il riesame del presente regolamento a norma dell'articolo 112, anche per quanto riguarda la comunicazione di incidenti gravi di cui all'articolo 73, e il funzionamento della banca dati dell'UE di cui all'articolo 71, la preparazione degli atti delegati o di esecuzione e gli eventuali allineamenti del presente regolamento alla normativa di armonizzazione elencata nell'allegato I;
 - iii) sulle specifiche tecniche o sulle norme esistenti relative ai requisiti di cui al capo III, sezione 2;
 - iv) sull'uso delle norme armonizzate o delle specifiche comuni di cui agli articoli 40 e 41;
 - v) sulle tendenze, quali la competitività globale europea nell'IA, l'adozione dell'IA nell'Unione e lo sviluppo di competenze digitali;
 - vi) sulle tendenze relative all'evoluzione della tipologia delle catene del valore dell'IA, in particolare per quanto riguarda le conseguenti implicazioni in termini di responsabilità;

- vii) sull'eventuale necessità di modificare l'allegato III conformemente all'articolo 7 e sull'eventuale necessità di una possibile revisione dell'articolo 5 a norma dell'articolo 112, tenendo conto delle pertinenti prove disponibili e degli ultimi sviluppi tecnologici;
- f) sostenere la Commissione nella promozione dell'alfabetizzazione in materia di IA, della sensibilizzazione del pubblico e della comprensione dei benefici, dei rischi, delle garanzie e dei diritti e degli obblighi in relazione all'uso dei sistemi di IA;
- g) facilitare lo sviluppo di criteri comuni e una comprensione condivisa tra gli operatori del mercato e le autorità competenti dei concetti pertinenti di cui al presente regolamento, anche contribuendo allo sviluppo di parametri di riferimento;
- h) cooperare, se del caso, con altre istituzioni e altri organi e organismi dell'Unione nonché con i pertinenti gruppi di esperti e reti dell'Unione, in particolare nei settori della sicurezza dei prodotti, della cibersicurezza, della concorrenza, dei servizi digitali e dei media, dei servizi finanziari, della protezione dei consumatori, dei dati e dei diritti fondamentali;
- i) contribuire all'efficace cooperazione con le autorità competenti dei paesi terzi e con le organizzazioni internazionali;
- j) assistere le autorità nazionali competenti e la Commissione nello sviluppo delle competenze organizzative e tecniche necessarie per l'attuazione del presente regolamento, anche contribuendo alla valutazione delle esigenze di formazione del personale degli Stati membri coinvolto nell'attuazione del presente regolamento;

- k) assistere l'ufficio per l'IA nel sostenere le autorità nazionali competenti nell'istituzione e nello sviluppo di spazi di sperimentazione normativa per l'IA e facilitare la cooperazione e la condivisione di informazioni tra gli spazi di sperimentazione normativa per l'IA;
- l) contribuire all'elaborazione di documenti di orientamento e fornire consulenza al riguardo;
- m) fornire consulenza alla Commissione sulle questioni internazionali in materia di IA;
- n) fornire pareri alla Commissione sulle segnalazioni qualificate relative ai modelli di IA per finalità generali;
- o) ricevere pareri dagli Stati membri sulle segnalazioni qualificate relative ai modelli di IA per finalità generali e sulle esperienze e pratiche nazionali in materia di monitoraggio e applicazione dei sistemi di IA, in particolare dei sistemi che integrano i modelli di IA per finalità generali.

Articolo 67

Forum consultivo

1. È istituito un forum consultivo per fornire consulenza e competenze tecniche al consiglio per l'IA e alla Commissione, nonché per contribuire ai loro compiti a norma del presente regolamento.
2. La composizione del forum consultivo rappresenta una selezione equilibrata di portatori di interessi, tra cui l'industria, le start-up, le PMI, la società civile e il mondo accademico. La composizione del forum consultivo è equilibrata per quanto riguarda gli interessi commerciali e non commerciali e, all'interno della categoria degli interessi commerciali, per quanto riguarda le PMI e le altre imprese.

3. La Commissione nomina i membri del forum consultivo, conformemente ai criteri stabiliti al paragrafo 2, tra i portatori di interessi con competenze riconosciute nel settore dell'IA.
4. Il mandato dei membri del forum consultivo ha una durata di due anni, prorogabile fino a un massimo di quattro anni.
5. L'Agenzia per i diritti fondamentali, l'ENISA, il Comitato europeo di normazione (CEN), il Comitato europeo di normazione elettrotecnica (CENELEC) e l'Istituto europeo per le norme di telecomunicazione (ETSI) sono membri permanenti del forum consultivo.
6. Il forum consultivo redige il proprio regolamento interno. Esso elegge due copresidenti tra i suoi membri, conformemente ai criteri stabiliti al paragrafo 2. Il mandato dei copresidenti ha una durata di due anni, rinnovabile una volta.
7. Il forum consultivo tiene riunioni almeno due volte all'anno. Il forum consultivo può invitare esperti e altri portatori di interessi alle sue riunioni.
8. Il forum consultivo può elaborare pareri, raccomandazioni e contributi scritti su richiesta del consiglio per l'IA o della Commissione.
9. Il forum consultivo può istituire sottogruppi permanenti o temporanei, se necessario, per esaminare questioni specifiche connesse agli obiettivi del presente regolamento.
10. Il forum consultivo prepara una relazione annuale sulle sue attività. Tale relazione è resa pubblica.

Articolo 68

Gruppo di esperti scientifici indipendenti

1. La Commissione adotta, mediante un atto di esecuzione, disposizioni sull'istituzione di un gruppo di esperti scientifici indipendenti ("gruppo di esperti scientifici") inteso a sostenere le attività di esecuzione a norma del presente regolamento. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.
2. Il gruppo di esperti scientifici è composto da esperti selezionati dalla Commissione sulla base di competenze scientifiche o tecniche aggiornate nel settore dell'IA necessarie per lo svolgimento dei compiti di cui al paragrafo 3 ed è in grado di dimostrare di soddisfare tutte le condizioni seguenti:
 - a) possesso di particolari conoscenze e capacità nonché competenze scientifiche o tecniche nel settore dell'IA;
 - b) indipendenza da qualsiasi fornitore di sistemi di IA o di modelli di IA per finalità generali;
 - c) capacità di svolgere attività in modo diligente, accurato e obiettivo.

La Commissione, in consultazione con il consiglio per l'IA, determina il numero di esperti del gruppo in funzione delle esigenze richieste e garantisce un'equa rappresentanza di genere e geografica.

3. Il gruppo di esperti scientifici fornisce consulenza e sostegno all'ufficio per l'IA, in particolare per quanto riguarda i compiti seguenti:
- a) sostenere l'attuazione e l'esecuzione del presente regolamento per quanto riguarda i modelli e i sistemi di IA per finalità generali, in particolare:
 - i) segnalare all'ufficio per l'IA i possibili rischi sistemici a livello dell'Unione dei modelli di IA per finalità generali, conformemente all'articolo 90;
 - ii) contribuire allo sviluppo di strumenti e metodologie per valutare le capacità dei modelli e sistemi di IA per finalità generali, anche attraverso parametri di riferimento;
 - iii) fornire consulenza sulla classificazione dei modelli di IA per finalità generali con rischio sistemico;
 - iv) fornire consulenza sulla classificazione di vari modelli e sistemi di IA per finalità generali;
 - v) contribuire allo sviluppo di strumenti e modelli;
 - b) sostenere il lavoro delle autorità di vigilanza del mercato, su richiesta di queste ultime;
 - c) sostenere le attività transfrontaliere di vigilanza del mercato di cui all'articolo 74, paragrafo 11, fatti salvi i poteri delle autorità di vigilanza del mercato;

- d) sostenere l'ufficio per l'IA nello svolgimento delle sue funzioni nell'ambito della procedura di salvaguardia dell'Unione di cui all'articolo 81.
4. Gli esperti scientifici del gruppo svolgono i loro compiti con imparzialità e obiettività e garantiscono la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività. Non sollecitano né accettano istruzioni da nessuno nell'esercizio dei loro compiti di cui al paragrafo 3. Ogni esperto compila una dichiarazione di interessi, che rende accessibile al pubblico. L'ufficio per l'IA istituisce sistemi e procedure per gestire attivamente e prevenire potenziali conflitti di interesse.
5. L'atto di esecuzione di cui al paragrafo 1 comprende disposizioni sulle condizioni, le procedure e le modalità dettagliate in base alle quali il gruppo di esperti scientifici e i suoi membri effettuano segnalazioni e chiedono l'assistenza dell'ufficio per l'IA per lo svolgimento dei compiti del gruppo di esperti scientifici.

Articolo 69

Accesso al gruppo di esperti da parte degli Stati membri

1. Gli Stati membri possono ricorrere agli esperti scientifici del gruppo affinché sostengano le loro attività di esecuzione a norma del presente regolamento.

2. Gli Stati membri possono essere tenuti a pagare tariffe per la consulenza e il sostegno forniti dagli esperti. La struttura e il livello delle tariffe, nonché l'entità e la struttura delle spese ripetibili sono indicati nell'atto di esecuzione di cui all'articolo 68, paragrafo 1, tenendo conto degli obiettivi di adeguata attuazione del presente regolamento, efficacia in termini di costi e necessità di garantire un accesso effettivo agli esperti per tutti gli Stati membri.
3. La Commissione facilita l'accesso tempestivo agli esperti da parte degli Stati membri, ove necessario, e garantisce che la combinazione di attività di sostegno svolte dalle strutture di sostegno dell'Unione per la prova dell'IA a norma dell'articolo 84 e dagli esperti a norma del presente articolo sia organizzata in modo efficiente e fornisca il miglior valore aggiunto possibile.

SEZIONE 2

AUTORITÀ NAZIONALI COMPETENTI

Articolo 70

Designazione delle autorità nazionali competenti e dei punti di contatto unici

1. Ciascuno Stato membro istituisce o designa come autorità nazionali competenti ai fini del presente regolamento almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato. Tali autorità nazionali competenti esercitano i loro poteri in modo indipendente, imparziale e senza pregiudizi, in modo da salvaguardare i principi di obiettività delle loro attività e dei loro compiti e garantire l'applicazione e l'attuazione del presente regolamento. I membri di tali autorità si astengono da qualsiasi atto incompatibile con le loro funzioni. A condizione che siano rispettati detti principi, tali compiti e attività possono essere svolti da una o più autorità designate, conformemente alle esigenze organizzative dello Stato membro.
2. Gli Stati membri comunicano alla Commissione l'identità delle autorità di notifica e delle autorità di vigilanza del mercato e i compiti di tali autorità, nonché ogni successiva modifica degli stessi. Gli Stati membri mettono a disposizione del pubblico le informazioni sulle modalità con cui le autorità competenti e i punti di contatto unici possono essere contattati, tramite mezzi di comunicazione elettronica, entro ... [12 mesi dalla data di entrata in vigore del presente regolamento]. Gli Stati membri designano un'autorità di vigilanza del mercato che funga da punto di contatto unico per il presente regolamento e notificano alla Commissione l'identità del punto di contatto unico. La Commissione elabora un elenco dei punti di contatto unici disponibili al pubblico.

3. Gli Stati membri garantiscono che le loro autorità nazionali competenti dispongano di risorse tecniche, finanziarie e umane adeguate, nonché delle infrastrutture necessarie per svolgere efficacemente i loro compiti a norma del presente regolamento. In particolare, le autorità nazionali competenti dispongono di sufficiente personale permanentemente disponibile, le cui competenze e conoscenze comprendono una comprensione approfondita delle tecnologie, dei dati e del calcolo dei dati di IA, della protezione dei dati personali, della cibersecurity, dei diritti fondamentali, dei rischi per la salute e la sicurezza e una conoscenza delle norme e dei requisiti giuridici esistenti. Gli Stati membri valutano e, se necessario, aggiornano annualmente i requisiti in termini di competenze e risorse di cui al presente paragrafo.
4. Le autorità nazionali competenti adottano misure adeguate per garantire un livello adeguato di cibersecurity.
5. Nello svolgimento dei propri compiti, le autorità nazionali competenti agiscono in conformità degli obblighi di riservatezza di cui all'articolo 78.
6. Entro ... [un anno dalla data di entrata in vigore del presente regolamento], e successivamente una volta ogni due anni, gli Stati membri riferiscono alla Commissione in merito allo stato delle risorse finanziarie e umane delle autorità nazionali competenti, con una valutazione della loro adeguatezza. La Commissione trasmette tali informazioni al consiglio per l'IA affinché le discuta e formuli eventuali raccomandazioni.
7. La Commissione agevola lo scambio di esperienze tra autorità nazionali competenti.

8. Le autorità nazionali competenti possono fornire orientamenti e consulenza sull'attuazione del presente regolamento, in particolare alle PMI, comprese le start-up, tenendo conto degli orientamenti e della consulenza del consiglio per l'IA e della Commissione, a seconda dei casi. Ogniquale volta le autorità nazionali competenti intendono fornire orientamenti e consulenza in relazione a un sistema di IA in settori disciplinati da altre disposizioni di diritto dell'Unione, sono consultate le autorità nazionali competenti a norma di tali disposizioni di diritto dell'Unione, come opportuno.
9. Qualora le istituzioni, gli organi e gli organismi dell'Unione rientrino nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità competente per la loro vigilanza.

Capo VIII

Banca dati dell'UE per i sistemi di IA ad alto rischio

Articolo 71

Banca dati dell'UE per i sistemi di IA ad alto rischio elencati nell'allegato III

1. La Commissione, in collaborazione con gli Stati membri, istituisce e mantiene una banca dati dell'UE contenente le informazioni di cui ai paragrafi 2 e 3 del presente articolo relative ai sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2, registrati conformemente agli articoli 49 e 60 e ai sistemi di IA che non sono considerati ad alto rischio a norma dell'articolo 6, paragrafo 3, e che sono registrati in conformità dell'articolo 6, paragrafo 4 e dell'articolo 69. Nel definire le specifiche funzionali di tale banca dati, la Commissione consulta gli esperti competenti e, nell'aggiornare le specifiche funzionali di tale banca dati, consulta il consiglio per l'IA.

2. I dati elencati nell'allegato VIII, sezioni A e B, sono inseriti nella banca dati dell'UE dal fornitore o, se del caso, dal rappresentante autorizzato.
3. I dati elencati nell'allegato VIII, sezione C, sono inseriti nella banca dati dell'UE dal deployer che è un'autorità, un'agenzia o un organismo pubblico, conformemente all'articolo 49, paragrafi 3 e 4, o che agisce per conto di essi.
4. Ad eccezione della sezione di cui all'articolo 49, paragrafo 4, e all'articolo 60, paragrafo 4, lettera c), le informazioni contenute nella banca dati dell'UE registrate a norma dell'articolo 49 sono accessibili e disponibili al pubblico in modo facilmente fruibile. Le informazioni dovrebbero essere di facile consultazione e leggibili meccanicamente. Le informazioni registrate a norma dell'articolo 60 sono accessibili solo alle autorità di vigilanza del mercato e alla Commissione, a meno che il fornitore o il potenziale fornitore non abbia dato il suo consenso anche a rendere tali informazioni accessibili al pubblico.
5. La banca dati dell'UE contiene dati personali solo nella misura necessaria per la raccolta e il trattamento delle informazioni in conformità del presente regolamento. Tali informazioni comprendono i nomi e i dati di contatto delle persone fisiche responsabili della registrazione del sistema e aventi l'autorità legale di rappresentare il fornitore o il deployer, se del caso.
6. La Commissione è il titolare del trattamento della banca dati dell'UE. Essa mette a disposizione dei fornitori, dei potenziali fornitori e dei deployer un adeguato sostegno tecnico e amministrativo. La banca dati dell'UE è conforme ai requisiti di accessibilità applicabili.

Capo IX

Monitoraggio successivo all'immissione sul mercato, condivisione delle informazioni e vigilanza del mercato

SEZIONE 1

MONITORAGGIO SUCCESSIVO ALL'IMMISSIONE SUL MERCATO

Articolo 72

*Monitoraggio successivo all'immissione sul mercato effettuato dai fornitori
e piano di monitoraggio successivo all'immissione sul mercato per i sistemi di IA ad alto rischio*

1. I fornitori istituiscono e documentano un sistema di monitoraggio successivo all'immissione sul mercato che sia proporzionato alla natura delle tecnologie di IA e ai rischi del sistema di IA ad alto rischio.
2. Il sistema di monitoraggio successivo all'immissione sul mercato raccoglie, documenta e analizza attivamente e sistematicamente i dati pertinenti che possono essere forniti dai deployer o che possono essere raccolti tramite altre fonti sulle prestazioni dei sistemi di IA ad alto rischio per tutta la durata del loro ciclo di vita e consente al fornitore di valutare la costante conformità dei sistemi di IA ai requisiti di cui al capo III, sezione 2. Se del caso, il monitoraggio successivo all'immissione sul mercato include un'analisi dell'interazione con altri sistemi di IA. Tale obbligo non riguarda i dati operativi sensibili dei deployer che sono autorità di contrasto.

3. Il sistema di monitoraggio successivo all'immissione sul mercato si basa su un piano di monitoraggio successivo all'immissione sul mercato. Il piano di monitoraggio successivo all'immissione sul mercato fa parte della documentazione tecnica di cui all'allegato IV. La Commissione adotta un atto di esecuzione che stabilisce disposizioni dettagliate in cui si definisce un modello per il piano di monitoraggio successivo all'immissione sul mercato e un elenco di elementi da includere nel piano entro ... [18 mesi dall'entrata in vigore del presente regolamento]. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

4. Per i sistemi di IA ad alto rischio disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, qualora tale normativa preveda già un sistema e un piano di monitoraggio successivo all'immissione sul mercato, al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari elementi di cui ai paragrafi 1, 2 e 3 utilizzando il modello di cui al paragrafo 3 nei sistemi e nei piani già esistenti in virtù di tale normativa, a condizione che consegua un livello di protezione equivalente.

Il primo comma del presente paragrafo si applica anche ai sistemi di IA ad alto rischio di cui all'allegato III, punto 5, immessi sul mercato o messi in servizio da istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari.

SEZIONE 2

CONDIVISIONE DI INFORMAZIONI SU INCIDENTI GRAVI

Articolo 73

Comunicazione di incidenti gravi

1. I fornitori di sistemi di IA ad alto rischio immessi sul mercato dell'Unione segnalano qualsiasi incidente grave alle autorità di vigilanza del mercato degli Stati membri in cui tali incidenti si sono verificati.
2. La segnalazione di cui al paragrafo 1 è effettuata immediatamente dopo che il fornitore ha stabilito un nesso causale tra il sistema di IA e l'incidente grave o quando stabilisce la ragionevole probabilità di tale nesso e, in ogni caso, non oltre 15 giorni dopo che il fornitore o, se del caso, il deployer, è venuto a conoscenza dell'incidente grave.

Il periodo per la segnalazione di cui al primo comma tiene conto della gravità dell'incidente grave.

3. In deroga al paragrafo 2 del presente articolo, in caso di un'infrazione diffusa o di un incidente grave quale definito all'articolo 3, punto 49, lettera b), la segnalazione di cui al paragrafo 1 del presente articolo è trasmessa immediatamente e non oltre due giorni dopo che il fornitore o, se del caso, il deployer è venuto a conoscenza di tale incidente.

4. In deroga al paragrafo 2, in caso di decesso di una persona, la segnalazione è trasmessa immediatamente dopo che il fornitore o il deployer ha stabilito, o non appena sospetta, un nesso causale tra il sistema di IA ad alto rischio e l'incidente grave, ma non oltre 10 giorni dalla data in cui il fornitore o, se del caso, il deployer è venuto a conoscenza dell'incidente grave.
5. Se necessario per garantire una comunicazione tempestiva, il fornitore o, se del caso, il deployer, può presentare una relazione iniziale incompleta, seguita da una relazione completa.
6. A seguito della comunicazione di un incidente grave a norma del paragrafo 1, il fornitore svolge senza indugio le indagini necessarie in relazione all'incidente grave e al sistema di IA interessato. Ciò comprende una valutazione del rischio dell'incidente nonché misure correttive.

Il fornitore coopera con le autorità competenti e, se del caso, con l'organismo notificato interessato durante le indagini di cui al primo comma e non svolge alcuna indagine che comporti una modifica del sistema di IA interessato in un modo che possa incidere su un'eventuale successiva valutazione delle cause dell'incidente, prima di informare le autorità competenti di tale azione.

7. Al ricevimento di una notifica relativa a un incidente grave di cui all'articolo 3, punto 49, lettera c), l'autorità di vigilanza del mercato interessata informa le autorità o gli organismi pubblici nazionali di cui all'articolo 77, paragrafo 1. La Commissione elabora orientamenti specifici per facilitare il rispetto degli obblighi di cui al paragrafo 1 del presente articolo. Tali orientamenti sono emanati entro ... [12 mesi dall'entrata in vigore del presente regolamento] e sono valutati periodicamente.

8. L'autorità di vigilanza del mercato adotta le misure appropriate di cui all'articolo 19 del regolamento (UE) 2019/1020 entro sette giorni dalla data di ricevimento della notifica di cui al paragrafo 1 del presente articolo e segue le procedure di notifica previste da tale regolamento.
9. Per i sistemi di IA ad alto rischio di cui all'allegato III che sono immessi sul mercato o messi in servizio da fornitori soggetti a strumenti legislativi dell'Unione che stabiliscono obblighi in materia di segnalazione equivalenti a quelli previsti dal presente regolamento, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 49, lettera c).
10. Per i sistemi di IA ad alto rischio che sono componenti di sicurezza di dispositivi, o sono essi stessi dispositivi, disciplinati dai regolamenti (UE) 2017/745 e (UE) 2017/746, la notifica è limitata agli incidenti gravi di cui all'articolo 3, punto 49, lettera c), del presente regolamento, del presente regolamento ed è trasmessa all'autorità nazionale competente scelta a tal fine dagli Stati membri in cui si è verificato l'incidente.
11. Le autorità nazionali competenti notificano immediatamente alla Commissione qualsiasi incidente grave, indipendentemente dal fatto che abbiano o meno preso provvedimenti al riguardo, conformemente all'articolo 20 del regolamento (UE) 2019/1020.

SEZIONE 3

APPLICAZIONE

Articolo 74

Vigilanza del mercato e controllo dei sistemi di IA nel mercato dell'Unione

1. Il regolamento (UE) 2019/1020 si applica ai sistemi di IA disciplinati dal presente regolamento. Ai fini dell'efficace applicazione del presente regolamento:
 - a) ogni riferimento a un operatore economico a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti gli operatori di cui all'articolo 2, paragrafo 1, del presente regolamento;
 - b) ogni riferimento a un prodotto a norma del regolamento (UE) 2019/1020 si intende fatto anche a tutti i sistemi di IA che rientrano nell'ambito di applicazione del presente regolamento.
2. Nell'ambito dei loro obblighi in materia di segnalazione a norma dell'articolo 34, paragrafo 4, del regolamento (UE) 2019/1020, le autorità di vigilanza del mercato comunicano annualmente alla Commissione e alle pertinenti autorità nazionali garanti della concorrenza qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per l'applicazione del diritto dell'Unione in materia di concorrenza. Essi riferiscono inoltre annualmente alla Commissione in merito al ricorso a pratiche vietate verificatosi nel corso di tale anno e alle misure adottate.
3. Per i sistemi di IA ad alto rischio collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità responsabile delle attività di vigilanza del mercato designata a norma di tali atti giuridici.

In deroga al primo comma e in determinate circostanze, gli Stati membri possono designare un'altra autorità pertinente che agisca in qualità di autorità di vigilanza del mercato, a condizione che garantiscano il coordinamento con le pertinenti autorità settoriali di vigilanza del mercato responsabili dell'esecuzione della normativa di armonizzazione dell'Unione elencata nell'allegato I.

4. Le procedure di cui agli articoli da 79 a 83 del presente regolamento non si applicano ai sistemi di IA collegati a prodotti disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, qualora tali atti giuridici prevedano già procedure che garantiscono un livello equivalente di protezione e aventi lo stesso obiettivo. In tali casi si applicano invece le pertinenti procedure settoriali.
5. Fatti salvi i poteri delle autorità di vigilanza del mercato di cui all'articolo 14 del regolamento (UE) 2019/1020, al fine di garantire l'efficace applicazione del presente regolamento, le autorità di vigilanza del mercato possono esercitare i poteri di cui all'articolo 14, paragrafo 4, lettere d) e j), di tale regolamento a distanza, se del caso.
6. Per i sistemi di IA ad alto rischio immessi sul mercato, messi in servizio o usati da istituti finanziari disciplinati dal diritto dell'Unione in materia di servizi finanziari, l'autorità di vigilanza del mercato ai fini del presente regolamento è l'autorità nazionale pertinente responsabile della vigilanza finanziaria di tali enti ai sensi di tale diritto, nella misura in cui l'immissione sul mercato, la messa in servizio o l'uso del sistema di IA siano direttamente collegati alla fornitura di tali servizi finanziari.

7. In deroga al paragrafo 6, in determinate circostanze e a condizione che sia garantito il coordinamento, lo Stato membro può individuare un'altra autorità competente come autorità di vigilanza del mercato ai fini del presente regolamento.

Le autorità nazionali di vigilanza del mercato che controllano gli enti creditizi disciplinati nel quadro della direttiva 2013/36/UE, che partecipano al meccanismo di vigilanza unico istituito dal regolamento (UE) n. 1024/2013, dovrebbero comunicare senza indugio alla Banca centrale europea qualsiasi informazione individuata nel corso delle attività di vigilanza del mercato che possa essere di potenziale interesse per i compiti in materia di vigilanza prudenziale della Banca centrale europea specificati in tale regolamento.

8. Per i sistemi di IA ad alto rischio elencati nell'allegato III del presente regolamento, punto 1, nella misura in cui tali sistemi sono utilizzati a fini di attività di contrasto, gestione delle frontiere, giustizia e democrazia e per i sistemi di IA ad alto rischio elencati nell'allegato III del presente regolamento, punti 6, 7 e 8, gli Stati membri designano come autorità di vigilanza del mercato ai fini del presente regolamento le autorità di controllo competenti per la protezione dei dati a norma del regolamento (UE) 2016/679 o della direttiva (UE) 2016/680 o qualsiasi altra autorità designata a norma delle stesse condizioni di cui agli articoli da 41 a 44 della direttiva (UE) 2016/680. Le attività di vigilanza del mercato non pregiudicano in alcun modo l'indipendenza delle autorità giudiziarie né interferiscono in altro modo con le loro attività nell'esercizio delle loro funzioni giurisdizionali.

9. Nei casi in cui le istituzioni, gli organi e gli organismi dell'Unione rientrano nell'ambito di applicazione del presente regolamento, il Garante europeo della protezione dei dati agisce in qualità di autorità di vigilanza del mercato, tranne nei confronti della Corte di giustizia dell'Unione europea nell'esercizio delle sue funzioni giurisdizionali.
10. Gli Stati membri agevolano il coordinamento tra le autorità di vigilanza del mercato designate a norma del presente regolamento e altre autorità o organismi nazionali pertinenti che controllano l'applicazione della normativa di armonizzazione dell'Unione elencata nell'allegato I o di altre disposizioni del diritto dell'Unione che potrebbero essere pertinenti per i sistemi di IA ad alto rischio di cui all'allegato III.
11. Le autorità di vigilanza del mercato e la Commissione possono proporre attività congiunte, comprese indagini congiunte, che dovrebbero essere condotte dalle autorità di vigilanza del mercato o dalle autorità di vigilanza del mercato di concerto con la Commissione, al fine di promuovere la conformità, individuare casi di non conformità, sensibilizzare e fornire orientamenti in relazione al presente regolamento riguardo a specifiche categorie di sistemi di IA ad alto rischio che si rileva presentino un rischio grave in due o più Stati membri conformemente all'articolo 9 del regolamento (UE) 2019/1020. L'ufficio per l'IA fornisce sostegno di coordinamento per le indagini congiunte.

12. Fatti salvi i poteri di cui al regolamento (UE) 2019/1020 e se del caso e nei limiti di quanto necessario per lo svolgimento dei loro compiti, i fornitori concedono alle autorità di vigilanza del mercato pieno accesso alla documentazione nonché ai set di dati di addestramento, convalida e prova utilizzati per lo sviluppo dei sistemi di IA ad alto rischio, anche, ove opportuno e fatte salve le garanzie di sicurezza, attraverso interfacce di programmazione delle applicazioni (API) o altri mezzi e strumenti tecnici pertinenti che consentano l'accesso remoto.
13. Alle autorità di vigilanza del mercato è concesso l'accesso al codice sorgente del sistema di IA ad alto rischio su richiesta motivata e solo qualora siano soddisfatte entrambe le condizioni seguenti:
- a) l'accesso al codice sorgente è necessario per valutare la conformità di un sistema di IA ad alto rischio ai requisiti di cui al capo III, sezione 2; e
 - b) le procedure di prova o di audit e le verifiche basate sui dati e sulla documentazione presentati dal fornitore sono state esaurite o si sono dimostrate insufficienti.
14. Qualsiasi informazione o documentazione ottenuta dalle autorità di vigilanza del mercato è trattata in conformità degli obblighi di riservatezza di cui all'articolo 78.

Articolo 75

Assistenza reciproca, vigilanza del mercato e controllo dei sistemi di IA per finalità generali

1. Qualora un sistema di IA si basi su un modello di IA per finalità generali e il modello e il sistema siano sviluppati dallo stesso fornitore, l'ufficio per l'IA ha il potere di monitorare e supervisionare la conformità di tale sistema di IA agli obblighi di cui al presente regolamento. Per svolgere i suoi compiti di monitoraggio e supervisione, l'ufficio per l'IA dispone di tutti i poteri di un'autorità di vigilanza del mercato prevista dalla presente sezione e dal regolamento (UE) 2019/1020.
2. Qualora abbiano motivi sufficienti per ritenere che i sistemi di IA per finalità generali che possono essere utilizzati direttamente dai deployer per almeno una finalità classificata come ad alto rischio a norma del presente regolamento non siano conformi ai requisiti di cui al presente regolamento, le pertinenti autorità di vigilanza del mercato cooperano con l'ufficio per l'IA per effettuare valutazioni della conformità e informano di conseguenza il consiglio per l'IA e le altre autorità di vigilanza del mercato.

3. Qualora non sia in grado di concludere la propria indagine sul sistema di IA ad alto rischio perché non può accedere a determinate informazioni relative al modello di IA per finalità generali nonostante abbia compiuto tutti gli sforzi opportuni per ottenere tali informazioni, un'autorità di vigilanza del mercato può presentare una richiesta motivata all'ufficio per l'IA, che garantisce l'accesso a tali informazioni. In tal caso, l'ufficio per l'IA fornisce all'autorità richiedente senza indugio, e in ogni caso entro 30 giorni, tutte le informazioni che esso ritiene pertinenti al fine di stabilire se un sistema di IA ad alto rischio non è conforme. Le autorità di vigilanza del mercato salvaguardano la riservatezza delle informazioni ottenute conformemente all'articolo 78 del presente regolamento. La procedura di cui al capo VI del regolamento (UE) 2019/1020 si applica *mutatis mutandis*.

Articolo 76

Controllo delle prove in condizioni reali da parte delle autorità di vigilanza del mercato

1. Le autorità di vigilanza del mercato hanno le competenze e i poteri per garantire che le prove in condizioni reali siano conformi al presente regolamento.
2. Qualora siano effettuate prove in condizioni reali per i sistemi di IA sottoposti a controllo all'interno di uno spazio di sperimentazione normativa per l'IA a norma dell'articolo 58, le autorità di vigilanza del mercato verificano la conformità dell'articolo 60 nell'ambito del loro ruolo di controllo per lo spazio di sperimentazione normativa per l'IA. Tali autorità possono, se del caso, consentire che le prove in condizioni reali siano effettuate dal fornitore o potenziale fornitore in deroga alle condizioni di cui all'articolo 60, paragrafo 4, lettere f) e g).

3. Qualora sia stata informata dal potenziale fornitore, dal fornitore o da un terzo di un incidente grave o abbia altri motivi per ritenere che le condizioni di cui agli articoli 60 e 61 non siano soddisfatte, un'autorità di vigilanza del mercato può adottare una delle seguenti decisioni sul suo territorio, a seconda dei casi:
 - a) sospendere o cessare le prove in condizioni reali;
 - b) imporre al fornitore o potenziale fornitore e al deployer o al potenziale deployer di modificare qualsiasi aspetto delle prove in condizioni reali.
4. Ove un'autorità di vigilanza del mercato abbia adottato una decisione di cui al paragrafo 3 o sollevato un'obiezione ai sensi dell'articolo 60, paragrafo 4, lettera b), la decisione o l'obiezione ne indica i motivi ed espone le modalità con cui il fornitore o potenziale fornitore può contestare la decisione o l'obiezione.
5. Se del caso, ove un'autorità di vigilanza del mercato abbia adottato una decisione di cui al paragrafo 3, ne comunica i motivi alle autorità di vigilanza del mercato degli altri Stati membri in cui il sistema di IA è stato sottoposto a prova conformemente al piano di prova.

Articolo 77

Poteri delle autorità che tutelano i diritti fondamentali

1. Le autorità o gli organismi pubblici nazionali che controllano o fanno rispettare gli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, compreso il diritto alla non discriminazione, in relazione all'uso dei sistemi di IA ad alto rischio di cui all'allegato III hanno il potere di richiedere qualsiasi documentazione creata o mantenuta a norma del presente regolamento o di accedervi, in una lingua e un formato accessibili, quando l'accesso a tale documentazione è necessario per l'efficace adempimento dei loro mandati entro i limiti della loro giurisdizione. L'autorità pubblica o l'organismo pubblico pertinente informa l'autorità di vigilanza del mercato dello Stato membro interessato di qualsiasi richiesta in tal senso.
2. Entro ... [tre mesi dall'entrata in vigore del presente regolamento], ciascuno Stato membro individua le autorità o gli organismi pubblici di cui al paragrafo 1 e ne pubblica l'elenco. Gli Stati membri notificano l'elenco alla Commissione e agli altri Stati membri e lo tengono aggiornato.
3. Qualora la documentazione di cui al paragrafo 1 non sia sufficiente per accertare un'eventuale violazione degli obblighi previsti dal diritto dell'Unione a tutela dei diritti fondamentali, l'autorità pubblica o l'organismo pubblico di cui al paragrafo 1 può presentare all'autorità di vigilanza del mercato una richiesta motivata al fine di organizzare una prova del sistema di IA ad alto rischio mediante mezzi tecnici. L'autorità di vigilanza del mercato organizza le prove coinvolgendo da vicino l'autorità pubblica o l'organismo pubblico richiedente entro un termine ragionevole dalla richiesta.

4. Qualsiasi informazione o documentazione ottenuta a norma del presente articolo dalle autorità o dagli organismi pubblici nazionali di cui al paragrafo 1 del presente articolo è trattata in conformità degli obblighi di riservatezza stabiliti all'articolo 78.

Articolo 78

Riservatezza

1. In conformità del diritto dell'Unione o nazionale, la Commissione, le autorità di vigilanza del mercato e gli organismi notificati, nonché le altre persone fisiche o giuridiche che partecipano all'applicazione del presente regolamento, garantiscono la riservatezza delle informazioni e dei dati ottenuti nello svolgimento dei loro compiti e delle loro attività in modo da tutelare, in particolare:
- a) i diritti di proprietà intellettuale e le informazioni commerciali riservate o i segreti commerciali di una persona fisica o giuridica, compreso il codice sorgente, tranne nei casi di cui all'articolo 5 della direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio¹⁷³;
 - b) l'efficace attuazione del presente regolamento, in particolare ai fini delle ispezioni, delle indagini e degli audit;
 - c) gli interessi pubblici e di sicurezza nazionale;
 - d) lo svolgimento del procedimento penale o amministrativo;
 - e) le informazioni classificate a norma del diritto dell'Unione o nazionale.

¹⁷³ Direttiva (UE) 2016/943 del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (GU L 157 del 15.6.2016, pag. 1).

2. Le autorità che partecipano all'applicazione del presente regolamento a norma del paragrafo 1 richiedono solo i dati strettamente necessari per la valutazione del rischio posto dai sistemi di IA e per l'esercizio dei loro poteri conformemente al presente regolamento e al regolamento (UE) 2019/1020. Esse pongono in essere misure di cibersicurezza adeguate ed efficaci per proteggere la sicurezza e la riservatezza delle informazioni e dei dati ottenuti e cancellano i dati raccolti non appena non sono più necessari per lo scopo per il quale sono stati ottenuti, conformemente al diritto dell'Unione o nazionale applicabile.
3. Fatti salvi i paragrafi 1 e 2, nel momento in cui i sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 o 7, sono utilizzati dalle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo, le informazioni scambiate in via riservata tra le autorità nazionali competenti, o tra le autorità nazionali competenti e la Commissione, non sono divulgate senza previa consultazione dell'autorità nazionale competente e del deployer che hanno prodotto tali informazioni, qualora tale divulgazione rischi di compromettere gli interessi pubblici e di sicurezza nazionale. Tale scambio di informazioni non riguarda i dati operativi sensibili in relazione alle attività delle autorità competenti in materia di contrasto, di controllo delle frontiere, di immigrazione o di asilo.

Qualora le autorità competenti in materia di contrasto, di immigrazione o di asilo siano fornitori di sistemi di IA ad alto rischio di cui all'allegato III, punti 1, 6 o 7, la documentazione tecnica di cui all'allegato IV rimane nei locali di tali autorità. Tali autorità garantiscono che le autorità di vigilanza del mercato di cui all'articolo 74, paragrafi 8 e 9, a seconda dei casi, possano, su richiesta, accedere immediatamente alla documentazione o ottenerne una copia. Solo il personale dell'autorità di vigilanza del mercato in possesso di un nulla osta di sicurezza di livello adeguato è autorizzato ad accedere a tale documentazione o a una copia della stessa.

4. I paragrafi 1, 2 e 3 non pregiudicano i diritti o gli obblighi della Commissione, degli Stati membri e delle rispettive autorità pertinenti nonché quelli degli organismi notificati in materia di scambio delle informazioni e di diffusione degli avvisi di sicurezza, anche nel contesto della cooperazione transfrontaliera, né pregiudicano gli obblighi delle parti interessate di fornire informazioni a norma del diritto penale degli Stati membri.
5. La Commissione e gli Stati membri possono scambiare, ove necessario e conformemente alle pertinenti disposizioni degli accordi internazionali e commerciali, informazioni riservate con le autorità di regolamentazione dei paesi terzi con i quali abbiano concluso accordi di riservatezza, bilaterali o multilaterali, che garantiscano un livello di riservatezza adeguato.

Articolo 79

Procedura a livello nazionale per i sistemi di IA che presentano un rischio

1. Un sistema di IA che presenta un rischio è inteso come un "prodotto che presenta un rischio" quale definito all'articolo 3, punto 19, del regolamento (UE) 2019/1020 nella misura in cui presenta rischi per la salute o la sicurezza o per i diritti fondamentali delle persone.

2. Qualora l'autorità di vigilanza del mercato di uno Stato membro abbia un motivo sufficiente per ritenere che un sistema di IA presenti un rischio di cui al paragrafo 1 del presente articolo, essa effettua una valutazione del sistema di IA interessato per quanto riguarda la sua conformità a tutti i requisiti e gli obblighi di cui al presente regolamento. Particolare attenzione è prestata ai sistemi di IA che presentano un rischio per i gruppi vulnerabili. Qualora siano individuati rischi per i diritti fondamentali, l'autorità di vigilanza del mercato informa anche le autorità o gli organismi pubblici nazionali competenti di cui all'articolo 77, paragrafo 1, e coopera pienamente con essi. I pertinenti operatori cooperano, per quanto necessario, con l'autorità di vigilanza del mercato e con le altre autorità o gli altri organismi pubblici nazionali di cui all'articolo 77, paragrafo 1.

Se, nel corso di tale valutazione, l'autorità di vigilanza del mercato o, se del caso, l'autorità di vigilanza del mercato in cooperazione con l'autorità pubblica nazionale di cui all'articolo 77, paragrafo 1, rilevano che il sistema di IA non è conforme ai requisiti e agli obblighi di cui al presente regolamento, esse chiedono senza indebito ritardo al pertinente operatore di adottare tutte le misure correttive adeguate al fine di rendere il sistema di IA conforme, ritirarlo dal mercato o richiamarlo entro il termine che l'autorità di vigilanza del mercato può prescrivere o, in ogni caso, entro 15 giorni lavorativi a seconda di quale termine sia il più breve, oppure entro il termine previsto dalla pertinente normativa di armonizzazione dell'Unione.

L'autorità di vigilanza del mercato informa di conseguenza l'organismo notificato pertinente. L'articolo 18 del regolamento (UE) 2019/1020 si applica alle misure di cui al secondo comma del presente paragrafo.

3. Qualora ritenga che la non conformità non sia limitata al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri senza indebito ritardo dei risultati della valutazione e delle azioni che hanno chiesto all'operatore economico di intraprendere.
4. L'operatore garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i sistemi di IA interessati che ha messo a disposizione sul mercato dell'Unione.
5. Qualora l'operatore di un sistema di IA non adotti misure correttive adeguate nel periodo di cui al paragrafo 2, l'autorità di vigilanza del mercato adotta tutte le misure provvisorie del caso per vietare o limitare la messa a disposizione o la messa in servizio del sistema di IA sul mercato nazionale, per ritirare il prodotto o il sistema di IA autonomo dal mercato o per richiamarlo. Tale autorità notifica senza indebito ritardo tali misure alla Commissione e agli altri Stati membri.
6. La notifica di cui al paragrafo 5 include tutti i particolari disponibili, soprattutto le informazioni necessarie all'identificazione del sistema di IA non conforme, la sua origine e la catena di approvvigionamento, la natura della presunta non conformità e dei rischi connessi, la natura e la durata delle misure nazionali adottate, nonché gli argomenti espressi dal pertinente operatore. Le autorità di vigilanza del mercato indicano in particolare se la non conformità sia dovuta a una o più delle cause seguenti:
 - a) non conformità al divieto delle pratiche di IA di cui all'articolo 5;
 - b) mancato rispetto da parte di un sistema di IA ad alto rischio dei requisiti di cui al capo III, sezione 2;

- c) carenze nelle norme armonizzate o nelle specifiche comuni, di cui agli articoli 40 e 41, che conferiscono la presunzione di conformità;
 - d) non conformità all'articolo 50.
7. Le autorità di vigilanza del mercato diverse dall'autorità di vigilanza del mercato dello Stato membro che ha avviato la procedura comunicano senza indebito ritardo alla Commissione e agli altri Stati membri tutte le misure adottate, tutte le altre informazioni a loro disposizione sulla non conformità del sistema di IA interessato e, in caso di disaccordo con la misura nazionale notificata, le loro obiezioni.
8. Se, entro tre mesi dal ricevimento della notifica di cui al paragrafo 5 del presente articolo, un'autorità di vigilanza del mercato di uno Stato membro o la Commissione non sollevano obiezioni contro la misura provvisoria adottata da un'autorità di vigilanza del mercato di un altro Stato membro, tale misura è ritenuta giustificata. Ciò non pregiudica i diritti procedurali dell'operatore interessato in conformità dell'articolo 18 del regolamento (UE) 2019/1020. Il periodo di tre mesi di cui al presente paragrafo è ridotto a 30 giorni in caso di non conformità al divieto delle pratiche di IA di cui all'articolo 5 del presente regolamento.
9. Le autorità di vigilanza del mercato garantiscono che siano adottate senza indebito ritardo adeguate misure restrittive in relazione al prodotto o al sistema di IA interessato, come il ritiro del prodotto o del sistema di IA dal loro mercato.

Articolo 80

Procedura per i sistemi di IA classificati dal fornitore come non ad alto rischio in applicazione dell'allegato III

1. Se ha motivi sufficienti per ritenere che un sistema di IA classificato dal fornitore come non ad alto rischio a norma dell'articolo 6, paragrafo 3, sia in realtà ad alto rischio, l'autorità di vigilanza del mercato effettua una valutazione del sistema di IA interessato in relazione alla sua classificazione come sistema di IA ad alto rischio sulla base delle condizioni di cui all'articolo 6, paragrafo 3, e degli orientamenti della Commissione.
2. Se, nel corso di tale valutazione, ritiene che il sistema di IA interessato sia ad alto rischio, l'autorità di vigilanza del mercato chiede senza indebito ritardo al fornitore pertinente di adottare tutte le misure necessarie per rendere il sistema di IA conforme ai requisiti e agli obblighi di cui al presente regolamento, nonché di adottare le opportune misure correttive entro un termine che l'autorità di vigilanza del mercato può prescrivere.
3. Se ritiene che l'uso del sistema di IA interessato non sia limitato al territorio nazionale, l'autorità di vigilanza del mercato informa la Commissione e gli altri Stati membri senza indebito ritardo dei risultati della valutazione e delle misure che ha chiesto al fornitore di adottare.

4. Il fornitore garantisce che siano adottate tutte le misure necessarie per rendere il sistema di IA conforme ai requisiti e agli obblighi di cui al presente regolamento. Qualora il fornitore di un sistema di IA interessato non renda il sistema di IA conforme a tali requisiti e obblighi entro il termine di cui al paragrafo 2 del presente articolo, il fornitore è soggetto a sanzioni pecuniarie conformemente all'articolo 99.
5. Il fornitore garantisce che siano adottate tutte le opportune misure correttive nei confronti di tutti i sistemi di IA interessati che ha messo a disposizione sul mercato dell'Unione.
6. Se il fornitore del sistema di IA in questione non adotta misure correttive adeguate entro il periodo di cui al paragrafo 2 del presente articolo, si applica l'articolo 79, paragrafi da 5 a 9.
7. Qualora, nel corso della valutazione di cui al paragrafo 1 del presente articolo, l'autorità di vigilanza del mercato stabilisca che il sistema di IA è stato classificato erroneamente dal fornitore come non ad alto rischio al fine di eludere l'applicazione dei requisiti di cui al capo III, sezione 2, il fornitore è soggetto a sanzioni pecuniarie conformemente all'articolo 99.
8. Nell'esercizio del loro potere di monitorare l'applicazione del presente articolo e in conformità dell'articolo 11 del regolamento (UE) 2019/1020, le autorità di vigilanza del mercato possono eseguire i controlli del caso, tenendo conto in particolare delle informazioni conservate nella banca dati dell'UE di cui all'articolo 71 del presente regolamento.

Articolo 81

Procedura di salvaguardia dell'Unione

1. Se entro tre mesi dal ricevimento della notifica di cui all'articolo 79, paragrafo 5, o entro 30 giorni in caso di non conformità al divieto delle pratiche di IA di cui all'articolo 5, l'autorità di vigilanza del mercato di uno Stato membro solleva obiezioni contro una misura adottata da un'altra autorità di vigilanza del mercato, o se la Commissione ritiene che la misura sia contraria al diritto dell'Unione, la Commissione consulta senza indebito ritardo l'autorità di vigilanza del mercato dello Stato membro interessato e l'operatore o gli operatori e valuta la misura nazionale. Sulla base dei risultati di tale valutazione, la Commissione, entro sei mesi, o entro 60 giorni in caso di non conformità al divieto delle pratiche di IA di cui all'articolo 5, a decorrere dalla notifica di cui all'articolo 79, paragrafo 5, decide se la misura nazionale sia giustificata e notifica la sua decisione all'autorità di vigilanza del mercato dello Stato membro interessato. La Commissione informa anche tutte le altre autorità di vigilanza del mercato della sua decisione.
2. Se la Commissione ritiene che la misura adottata dallo Stato membro interessato sia giustificata, tutti gli Stati membri provvedono ad adottare misure restrittive appropriate in relazione al sistema di IA interessato, ad esempio richiedendo il ritiro del sistema di IA dal loro mercato senza indebito ritardo, e ne informano la Commissione. Se la Commissione ritiene che la misura nazionale sia ingiustificata, lo Stato membro interessato provvede a ritirarla e ne informa la Commissione.

3. Se la misura nazionale è ritenuta giustificata e la non conformità del sistema di IA è attribuita alle carenze nelle norme armonizzate o nelle specifiche comuni di cui agli articoli 40 e 41 del presente regolamento, la Commissione applica la procedura prevista all'articolo 11 del regolamento (UE) n. 1025/2012.

Articolo 82

Sistemi di IA conformi che presentano un rischio

1. Se, dopo aver effettuato una valutazione a norma dell'articolo 79 e aver consultato la pertinente autorità pubblica nazionale di cui all'articolo 77, paragrafo 1, l'autorità di vigilanza del mercato di uno Stato membro ritiene che un sistema di IA ad alto rischio, pur conforme al presente regolamento, rappresenti comunque un rischio per la salute o la sicurezza delle persone, per i diritti fondamentali o per altri aspetti della tutela dell'interesse pubblico, essa chiede all'operatore pertinente di adottare tutte le misure adeguate a far sì che il sistema di IA in questione, all'atto della sua immissione sul mercato o messa in servizio, non presenti più tale rischio senza indebito ritardo entro un termine che essa può prescrivere.
2. Il fornitore o un altro operatore pertinente garantisce l'adozione di misure correttive nei confronti di tutti i sistemi di IA interessati che ha messo a disposizione sul mercato dell'Unione entro il termine prescritto dall'autorità di vigilanza del mercato dello Stato membro di cui al paragrafo 1.

3. Gli Stati membri informano immediatamente la Commissione e gli altri Stati membri della conclusione cui sono giunti conformemente al paragrafo 1. Tali informazioni comprendono tutti i dettagli disponibili, in particolare i dati necessari all'identificazione del sistema di IA interessato, l'origine e la catena di approvvigionamento del sistema di IA, la natura del rischio connesso, nonché la natura e la durata delle misure nazionali adottate.
4. La Commissione avvia senza indebito ritardo consultazioni con gli Stati membri interessati e gli operatori pertinenti e valuta le misure nazionali adottate. In base ai risultati di tale valutazione, la Commissione decide se la misura sia giustificata e propone, ove necessario, altre misure appropriate.
5. La Commissione comunica immediatamente la propria decisione agli Stati membri interessati e agli operatori pertinenti e ne informa anche gli altri Stati membri.

Articolo 83

Non conformità formale

1. L'autorità di vigilanza del mercato di uno Stato membro chiede al fornitore pertinente, entro un termine che essa può prescrivere, di porre fine alla contestata non conformità qualora giunga a una delle conclusioni riportate di seguito:
 - a) la marcatura CE è stata apposta in violazione dell'articolo 48;
 - b) la marcatura CE non è stata apposta;
 - c) la dichiarazione di conformità UE di cui all'articolo 47 non è stata redatta;

- d) la dichiarazione di conformità UE di cui all'articolo 47 non è stata redatta correttamente;
 - e) la registrazione nella banca dati dell'UE di cui all'articolo 71 non è stata effettuata;
 - f) se del caso, non è stato nominato nessun rappresentante autorizzato;
 - g) la documentazione tecnica non è disponibile.
2. Se la non conformità di cui al paragrafo 1 permane, l'autorità di vigilanza del mercato dello Stato membro interessato adotta misure appropriate e proporzionate per limitare o proibire la messa a disposizione sul mercato del sistema di IA ad alto rischio o per garantire che sia richiamato o ritirato dal mercato senza ritardo.

Articolo 84

Strutture di sostegno dell'Unione per la prova dell'IA

1. La Commissione designa una o più strutture di sostegno dell'Unione per la prova dell'IA per lo svolgimento dei compiti di cui all'articolo 21, paragrafo 6, del regolamento (UE) 2019/1020/nel settore dell'IA.
2. Fatti salvi i compiti di cui al paragrafo 1, le strutture di sostegno dell'Unione per la prova dell'IA forniscono anche pareri tecnici o scientifici indipendenti su richiesta del consiglio per l'IA, della Commissione o delle autorità di vigilanza del mercato.

SEZIONE 4

MEZZI DI RICORSO

Articolo 85

Diritto di presentare un reclamo a un'autorità di vigilanza del mercato

Fatti salvi altri ricorsi amministrativi o giurisdizionali, qualsiasi persona fisica o giuridica che abbia motivo di ritenere che vi sia stata una violazione delle disposizioni del presente regolamento può presentare un reclamo alla pertinente autorità di vigilanza del mercato.

Conformemente al regolamento (UE) 2019/1020, tali reclami sono presi in considerazione ai fini dello svolgimento delle attività di vigilanza del mercato e sono trattati in linea con le procedure specifiche stabilite a tal fine dalle autorità di vigilanza del mercato.

Articolo 86

Diritto alla spiegazione dei singoli processi decisionali

1. Qualsiasi persona interessata oggetto di una decisione adottata dal deployer sulla base dell'output di un sistema di IA ad alto rischio elencato nell'allegato III, ad eccezione dei sistemi elencati al punto 2 dello stesso, e che produca effetti giuridici o in modo analogo incida significativamente su tale persona in un modo che essa ritenga avere un impatto negativo sulla sua salute, sulla sua sicurezza o sui suoi diritti fondamentali ha il diritto di ottenere dal deployer spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata.

2. Il paragrafo 1 non si applica all'uso di sistemi di IA per i quali sono previste eccezioni o limitazioni all'obbligo stabilito in tale paragrafo in virtù del diritto dell'Unione o del diritto nazionale, in linea con il diritto dell'Unione.
3. Il presente articolo si applica solo nella misura in cui il diritto di cui al paragrafo 1 non sia altrimenti previsto dal diritto dell'Unione.

Articolo 87

Segnalazione delle violazioni e protezione delle persone segnalanti

La direttiva (UE) 2019/1937 si applica alla segnalazione di violazioni del presente regolamento e alla protezione delle persone che segnalano tali violazioni.

SEZIONE 5

SUPERVISIONE, INDAGINI, ESECUZIONE E MONITORAGGIO IN RELAZIONE AI FORNITORI DI MODELLI DI IA PER FINALITÀ GENERALI

Articolo 88

Esecuzione degli obblighi dei fornitori di modelli di IA per finalità generali

1. La Commissione ha competenze esclusive per la vigilanza e l'esecuzione del capo V, tenendo conto delle garanzie procedurali a norma all'articolo 94. La Commissione affida l'attuazione di tali compiti all'ufficio per l'IA, fatte salve le competenze di organizzazione della Commissione e la ripartizione delle competenze tra gli Stati membri e l'Unione sulla base dei trattati.

2. Fatto salvo l'articolo 75, paragrafo 3, le autorità di vigilanza del mercato possono chiedere alla Commissione di esercitare le competenze di cui alla presente sezione, ove ciò sia necessario e proporzionato per assisterle nell'adempimento dei loro compiti a norma del presente regolamento.

Articolo 89

Azioni di monitoraggio

1. Ai fini dello svolgimento dei compiti ad esso assegnati a norma della presente sezione, l'ufficio per l'IA può intraprendere le azioni necessarie per monitorare l'efficace attuazione e il rispetto del presente regolamento da parte dei fornitori di modelli di IA per finalità generali, compresa la loro adesione ai codici di buone pratiche approvati.
2. I fornitori a valle hanno il diritto di presentare un reclamo per presunta violazione del presente regolamento. Il reclamo è debitamente motivato e indica almeno:
 - a) il punto di contatto del fornitore del modello di IA per finalità generali in questione;
 - b) una descrizione dei fatti di cui trattasi, delle pertinenti disposizioni del presente regolamento e del motivo per cui il fornitore a valle ritiene che il fornitore del modello di IA per finalità generali in questione abbia violato il presente regolamento;
 - c) qualsiasi altra informazione che il fornitore a valle che ha inviato la richiesta ritenga pertinente, comprese, se del caso, le informazioni raccolte di propria iniziativa.

Articolo 90

Segnalazioni di rischi sistemici da parte del gruppo di esperti scientifici

1. Il gruppo di esperti scientifici può effettuare una segnalazione qualificata all'ufficio per l'IA qualora abbia motivo di sospettare che:
 - a) un modello di IA per finalità generali presenti un rischio concreto identificabile a livello dell'Unione; o
 - b) un modello di IA per finalità generali soddisfi le condizioni di cui all'articolo 51.
2. In seguito a tale segnalazione qualificata, la Commissione, tramite l'ufficio per l'IA e dopo avere informato il consiglio per l'IA, può esercitare le competenze di cui alla presente sezione ai fini della valutazione della questione. L'ufficio per l'IA informa il consiglio per l'IA di qualsiasi misura conformemente agli articoli da 91 a 94.
3. La segnalazione qualificata è debitamente motivata e indica almeno:
 - a) il punto di contatto del fornitore del modello di IA per finalità generali con rischio sistemico in questione;
 - b) una descrizione dei fatti di cui trattasi e dei motivi della segnalazione effettuata dal gruppo di esperti scientifici;
 - c) qualsiasi altra informazione che il gruppo di esperti scientifici ritenga pertinente, comprese, se del caso, le informazioni raccolte di propria iniziativa.

Articolo 91

Potere di richiedere documentazione e informazioni

1. La Commissione può chiedere al fornitore del modello di IA per finalità generali in questione di fornire la documentazione redatta dal fornitore in conformità degli articoli 53 e 55 o qualsiasi altra informazione supplementare necessaria al fine di valutare la conformità del fornitore al presente regolamento.
2. Prima di inviare la richiesta di informazioni, l'ufficio per l'IA può avviare un dialogo strutturato con il fornitore del modello di IA per finalità generali.
3. Su richiesta debitamente motivata del gruppo di esperti scientifici, la Commissione può presentare una richiesta di informazioni a un fornitore di un modello di IA per finalità generali, qualora l'accesso alle informazioni sia necessario e proporzionato per l'adempimento dei compiti del gruppo di esperti scientifici a norma dell'articolo 68, paragrafo 2.
4. La richiesta di informazioni indica la base giuridica e lo scopo della richiesta, precisa quali informazioni sono richieste, fissa un termine entro il quale le informazioni devono essere fornite e indica le sanzioni pecuniarie previste all'articolo 101 in caso di comunicazione di informazioni inesatte, incomplete o fuorvianti.

5. Il fornitore del modello di IA per finalità generali in questione o il suo rappresentante fornisce le informazioni richieste. Nel caso di persone giuridiche, società o imprese, o qualora il fornitore non abbia personalità giuridica, le persone autorizzate a rappresentarle per legge o in virtù del loro statuto forniscono le informazioni richieste per conto del fornitore del modello di IA per finalità generali in questione. Gli avvocati debitamente incaricati possono fornire le informazioni per conto dei loro clienti. I clienti restano tuttavia pienamente responsabili se le informazioni fornite sono incomplete, inesatte o fuorvianti.

Articolo 92

Potere di effettuare valutazioni

1. L'ufficio per l'IA, previa consultazione del consiglio per l'IA, può effettuare valutazioni del modello di IA per finalità generali in questione:
- a) per valutare la conformità del fornitore agli obblighi previsti dal presente regolamento, qualora le informazioni raccolte a norma dell'articolo 91 siano insufficienti; o
 - b) per indagare sui rischi sistemici a livello dell'Unione dei modelli di IA per finalità generali con rischio sistemico, in particolare a seguito di una segnalazione qualificata del gruppo di esperti scientifici conformemente all'articolo 90, paragrafo 1, lettera a).
2. La Commissione può decidere di nominare esperti indipendenti incaricati di effettuare valutazioni per suo conto, anche provenienti dal gruppo di esperti scientifici istituito a norma dell'articolo 68. Gli esperti indipendenti nominati per tale compito soddisfano i criteri di cui all'articolo 68, paragrafo 2.

3. Ai fini del paragrafo 1, la Commissione può chiedere l'accesso al modello di IA per finalità generali in questione attraverso API o altri mezzi e strumenti tecnici adeguati, compreso il codice sorgente.
4. La richiesta di accesso indica la base giuridica, lo scopo e i motivi della richiesta e fissa il termine entro il quale deve essere fornito l'accesso e le sanzioni pecuniarie previste all'articolo 101 in caso di mancata fornitura dell'accesso.
5. I fornitori del modello di IA per finalità generali in questione o il loro rappresentante forniscono le informazioni richieste. Nel caso di persone giuridiche, società o imprese, o qualora i fornitori non abbiano personalità giuridica, le persone autorizzate a rappresentarli per legge o in virtù del loro statuto, forniscono l'accesso richiesto per conto del fornitore del modello di IA per finalità generali in questione.
6. La Commissione adotta atti di esecuzione che stabiliscono le modalità dettagliate e le condizioni per le valutazioni, comprese le modalità dettagliate per la partecipazione di esperti indipendenti, nonché la procedura per la loro selezione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.
7. Prima di richiedere l'accesso al modello di IA per finalità generali in questione, l'ufficio per l'IA può avviare un dialogo strutturato con il fornitore del modello di IA per finalità generali al fine di raccogliere maggiori informazioni sulle prove interne del modello, sulle garanzie interne per prevenire rischi sistemici e su altre procedure e misure interne che il fornitore ha adottato per attenuare tali rischi.

Articolo 93
Potere di richiedere misure

1. Se necessario e opportuno, la Commissione può chiedere ai fornitori di:
 - a) adottare misure adeguate per adempiere gli obblighi di cui agli articoli 53 e 54;
 - b) attuare misure di attenuazione se la valutazione effettuata conformemente all'articolo 92 ha suscitato un timore serio e comprovato di un rischio sistemico a livello dell'Unione;
 - c) limitare la messa a disposizione sul mercato, ritirare o richiamare il modello.
2. Prima di richiedere una misura, l'ufficio per l'IA può avviare un dialogo strutturato con il fornitore del modello di IA per finalità generali.
3. Se, durante il dialogo strutturato di cui al paragrafo 2, il fornitore del modello di IA per finalità generali con rischio sistemico si assume impegni relativi all'attuazione di misure di attenuazione per far fronte a un rischio sistemico a livello dell'Unione, la Commissione può, mediante decisione, rendere tali impegni vincolanti e dichiarare che non vi sono ulteriori motivi di intervento.

Articolo 94

Diritti procedurali degli operatori economici del modello di IA per finalità generali

L'articolo 18 del regolamento (UE) 2019/1020 si applica mutatis mutandis ai fornitori del modello di IA per finalità generali, fatti salvi i diritti procedurali più specifici previsti dal presente regolamento.

Capo X

Codici di condotta e orientamenti

Articolo 95

Codici di condotta per l'applicazione volontaria di requisiti specifici

1. L'ufficio per l'IA e gli Stati membri incoraggiano e agevolano l'elaborazione di codici di condotta, compresi i relativi meccanismi di governance, intesi a promuovere l'applicazione volontaria ai sistemi di IA, diversi dai sistemi di IA ad alto rischio, di alcuni o di tutti i requisiti di cui al capo III, sezione 2, tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore che consentono l'applicazione di tali requisiti.

2. L'ufficio per l'IA e gli Stati membri agevolano l'elaborazione di codici di condotta relativi all'applicazione volontaria, anche da parte dei deployer, di requisiti specifici a tutti i sistemi di IA, sulla base di obiettivi chiari e indicatori chiave di prestazione volti a misurare il conseguimento di tali obiettivi, compresi elementi quali, a titolo puramente esemplificativo:
- a) gli elementi applicabili previsti negli orientamenti etici dell'Unione per un'IA affidabile;
 - b) la valutazione e la riduzione al minimo dell'impatto dei sistemi di IA sulla sostenibilità ambientale, anche per quanto riguarda la programmazione efficiente sotto il profilo energetico e le tecniche per la progettazione, l'addestramento e l'uso efficienti dell'IA;
 - c) la promozione dell'alfabetizzazione in materia di IA, in particolare quella delle persone che si occupano dello sviluppo, del funzionamento e dell'uso dell'IA;
 - d) la facilitazione di una progettazione inclusiva e diversificata dei sistemi di IA, anche attraverso la creazione di gruppi di sviluppo inclusivi e diversificati e la promozione della partecipazione dei portatori di interessi a tale processo;
 - e) la valutazione e la prevenzione dell'impatto negativo dei sistemi di IA sulle persone vulnerabili o sui gruppi di persone vulnerabili, anche per quanto riguarda l'accessibilità per le persone con disabilità, nonché sulla parità di genere.

3. I codici di condotta possono essere elaborati da singoli fornitori o deployer di sistemi di IA o da organizzazioni che li rappresentano o da entrambi, anche con la partecipazione di qualsiasi portatore di interessi e delle sue organizzazioni rappresentative, comprese le organizzazioni della società civile e il mondo accademico. I codici di condotta possono riguardare uno o più sistemi di IA tenendo conto della similarità della finalità prevista dei sistemi pertinenti.
4. Nell'incoraggiare e agevolare l'elaborazione dei codici di condotta, l'ufficio per l'IA e gli Stati membri tengono conto degli interessi e delle esigenze specifici delle PMI, comprese le start-up.

Articolo 96

Orientamenti della Commissione sull'attuazione del regolamento

1. La Commissione elabora orientamenti sull'attuazione pratica del presente regolamento, in particolare per quanto riguarda:
 - a) l'applicazione dei requisiti e degli obblighi di cui agli articoli da 8 a 15 e all'articolo 25;
 - b) le pratiche vietate di cui all'articolo 5;
 - c) l'attuazione pratica delle disposizioni relative alla modifica sostanziale;
 - d) l'attuazione pratica degli obblighi di trasparenza di cui all'articolo 50;

- e) informazioni dettagliate sulla relazione del presente regolamento con la normativa di armonizzazione dell'Unione elencata nell'allegato I, nonché con altre disposizioni pertinenti di diritto dell'Unione, anche per quanto riguarda la coerenza nella loro applicazione;
- f) l'applicazione della definizione di sistema di IA di cui all'articolo 3, punto 1).

Quando pubblica tali orientamenti, la Commissione presta particolare attenzione alle esigenze delle PMI, comprese le start-up, delle autorità pubbliche locali e dei settori maggiormente interessati dal presente regolamento.

Gli orientamenti di cui al primo comma del presente paragrafo tengono debitamente conto dello stato dell'arte generalmente riconosciuto in materia di IA, nonché delle pertinenti norme armonizzate e specifiche comuni di cui agli articoli 40 e 41, o delle norme armonizzate o specifiche tecniche stabilite a norma della normativa di armonizzazione dell'Unione.

2. Su richiesta degli Stati membri o dell'ufficio per l'IA, o di propria iniziativa, la Commissione aggiorna gli orientamenti adottati quando lo ritiene necessario.

Capo XI

Delega di potere e procedura di comitato

Articolo 97

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.
2. Il potere di adottare atti delegati di cui all'articolo 6, paragrafi 6 e 7, all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, all'articolo 47, paragrafo 5, all'articolo 51, paragrafo 3, all'articolo 52, paragrafo 4, e all'articolo 53, paragrafi 5 e 6, è conferito alla Commissione per un periodo di cinque anni a decorrere dal ... [data di entrata in vigore del presente regolamento]. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo di cinque anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.
3. La delega di potere di cui all'articolo 6, paragrafi 6 e 7, all'articolo 7, paragrafi 1 e 3, all'articolo 11, paragrafo 3, all'articolo 43, paragrafi 5 e 6, all'articolo 47, paragrafo 5, all'articolo 51, paragrafo 3, all'articolo 52, paragrafo 4, e all'articolo 53, paragrafi 5 e 6, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.
5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.
6. Qualsiasi atto delegato adottato a norma dell'articolo 6, paragrafi 6 o 7, dell'articolo 7, paragrafi 1 o 3, dell'articolo 11, paragrafo 3, dell'articolo 43, paragrafi 5 o 6, dell'articolo 47, paragrafo 5, dell'articolo 51, paragrafo 3, dell'articolo 52, paragrafo 4, o dell'articolo 53, paragrafi 5 o 6, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 98

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Capo XII

Sanzioni

Articolo 99

Sanzioni

1. In conformità dei termini e delle condizioni di cui al presente regolamento, gli Stati membri stabiliscono le norme relative alle sanzioni e alle altre misure di esecuzione, che possono includere anche avvertimenti e misure non pecuniarie, applicabili in caso di violazione del presente regolamento da parte degli operatori, e adottano tutte le misure necessarie per garantirne un'attuazione corretta ed efficace, tenendo conto degli orientamenti emanati dalla Commissione a norma dell'articolo 96. Le sanzioni previste sono effettive, proporzionate e dissuasive. Esse tengono conto degli interessi delle PMI, comprese le start-up, e della loro sostenibilità economica.
2. Gli Stati membri notificano alla Commissione, senza indugio e al più tardi entro la data di entrata in applicazione, le norme relative alle sanzioni e le altre misure di esecuzione di cui al paragrafo 1, e provvedono poi a dare immediata notifica delle eventuali modifiche successive.
3. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 35 000 000 EUR o, se l'autore del reato è un'impresa, fino al 7 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4. La non conformità a qualsiasi delle seguenti disposizioni connesse a operatori o organismi notificati, diverse da quelle di cui all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 15 000 000 EUR o, se l'autore del reato è un'impresa, fino al 3 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:
- a) gli obblighi dei fornitori a norma dell'articolo 16;
 - b) gli obblighi dei rappresentanti autorizzati a norma dell'articolo 22;
 - c) gli obblighi degli importatori a norma dell'articolo 23;
 - d) gli obblighi dei distributori a norma dell'articolo 24;
 - e) gli obblighi dei deployer a norma dell'articolo 26;
 - f) i requisiti e gli obblighi degli organismi notificati a norma dell'articolo 31, dell'articolo 33, paragrafi 1, 3 e 4, o dell'articolo 34;
 - g) gli obblighi di trasparenza per i fornitori e i deployers a norma dell'articolo 50.
5. La fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti per dare seguito a una richiesta è soggetta a sanzioni amministrative pecuniarie fino a 7 500 000 EUR o, se l'autore del reato è un'impresa, fino all'1 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.
6. Nel caso delle PMI, comprese le start-up, ciascuna sanzione pecuniaria di cui al presente articolo è pari al massimo alle percentuali o all'importo di cui ai paragrafi 3, 4 e 5, se inferiore.

7. Nel decidere se infliggere una sanzione amministrativa pecuniaria e nel determinarne l'importo in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e, se del caso, si tiene in considerazione quanto segue:
- a) la natura, la gravità e la durata della violazione e delle sue conseguenze, tenendo in considerazione la finalità del sistema di IA, nonché, ove opportuno, il numero di persone interessate e il livello del danno da esse subito;
 - b) se altre autorità di vigilanza del mercato hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per la stessa violazione;
 - c) se altre autorità hanno già applicato sanzioni amministrative pecuniarie allo stesso operatore per violazioni di altre disposizioni del diritto dell'Unione o nazionale, qualora tali violazioni derivino dalla stessa attività o omissione che costituisce una violazione pertinente del presente regolamento;
 - d) le dimensioni, il fatturato annuo e la quota di mercato dell'operatore che ha commesso la violazione;
 - e) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione;
 - f) il grado di cooperazione con le autorità nazionali competenti al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

- g) il grado di responsabilità dell'operatore tenendo conto delle misure tecniche e organizzative attuate;
 - h) il modo in cui le autorità nazionali competenti sono venute a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'operatore;
 - i) il carattere doloso o colposo della violazione;
 - j) l'eventuale azione intrapresa dall'operatore per attenuare il danno subito dalle persone interessate.
8. Ciascuno Stato membro può prevedere norme che dispongano in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.
9. A seconda dell'ordinamento giuridico degli Stati membri, le norme in materia di sanzioni amministrative pecuniarie possono essere applicate in modo tale che le sanzioni pecuniarie siano inflitte dalle autorità giudiziarie nazionali competenti o da altri organismi, quali applicabili in tali Stati membri. L'applicazione di tali norme in tali Stati membri ha effetto equivalente.
10. L'esercizio dei poteri attribuiti dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e nazionale, inclusi il ricorso giurisdizionale effettivo e il giusto processo.
11. Gli Stati membri riferiscono annualmente alla Commissione in merito alle sanzioni amministrative pecuniarie inflitte nel corso dell'anno, in conformità del presente articolo, e a eventuali controversie o procedimenti giudiziari correlati.

Articolo 100

Sanzioni amministrative pecuniarie inflitte a istituzioni, organi e organismi dell'Unione

1. Il Garante europeo della protezione dei dati può infliggere sanzioni amministrative pecuniarie alle istituzioni, agli organi e agli organismi dell'Unione che rientrano nell'ambito di applicazione del presente regolamento. Nel decidere se infliggere una sanzione amministrativa pecuniaria e nel determinarne l'importo in ogni singolo caso, si tiene conto di tutte le circostanze pertinenti della situazione specifica e si tiene quanto segue in debita considerazione:
 - a) la natura, la gravità e la durata della violazione e delle sue conseguenze, tenendo in considerazione la finalità del sistema di IA interessato, nonché se del caso, il numero di persone interessate e il livello del danno da esse subito;
 - b) il grado di responsabilità dell'istituzione, dell'organo o dell'organismo dell'Unione, tenendo conto delle misure tecniche e organizzative da essi attuate;
 - c) qualsiasi azione intrapresa dall'istituzione, dall'organo o dall'organismo dell'Unione per attenuare il danno subito dalle persone interessate;
 - d) il grado di cooperazione con il Garante europeo della protezione dei dati al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi, compreso il rispetto delle misure precedentemente disposte dal Garante europeo della protezione dei dati nei confronti dell'istituzione, dell'organo o dell'organismo dell'Unione interessato in relazione allo stesso tema;

- e) eventuali precedenti violazioni analoghe commesse dall'istituzione, dall'organo o dall'organismo dell'Unione;
 - f) il modo in cui il Garante europeo della protezione dei dati è venuto a conoscenza della violazione, in particolare se e in che misura è stata notificata dall'istituzione, dall'organo o dall'organismo dell'Unione;
 - g) il bilancio annuale dell'istituzione, dell'organo o dell'organismo dell'Unione.
2. La non conformità al divieto delle pratiche di IA di cui all'articolo 5 è soggetta a sanzioni amministrative pecuniarie fino a 1 500 000 EUR.
 3. La non conformità del sistema di IA ai requisiti o agli obblighi a norma del presente regolamento, diversi da quelli previsti all'articolo 5, è soggetta a sanzioni amministrative pecuniarie fino a 750 000 EUR.
 4. Prima di adottare qualsiasi decisione a norma del presente articolo, il Garante europeo della protezione dei dati dà all'istituzione, all'organo o all'organismo dell'Unione oggetto del procedimento avviato dal Garante europeo della protezione dei dati l'opportunità di esprimersi in merito all'eventuale violazione. Il Garante europeo della protezione dei dati basa le sue decisioni solo sugli elementi e le circostanze in merito ai quali le parti interessate sono state poste in condizione di esprimersi. Gli eventuali ricorrenti sono strettamente associati al procedimento.

5. Nel corso del procedimento sono pienamente garantiti i diritti di difesa delle parti interessate. Esse hanno diritto d'accesso al fascicolo del Garante europeo della protezione dei dati, fermo restando l'interesse legittimo delle persone fisiche o delle imprese alla tutela dei propri dati personali o segreti aziendali.
6. I fondi raccolti mediante l'imposizione di sanzioni pecuniarie in forza del presente articolo contribuiscono al bilancio generale dell'Unione. Le sanzioni pecuniarie non pregiudicano l'effettivo funzionamento dell'istituzione, dell'organo o dell'organismo dell'Unione sanzionato.
7. Il Garante europeo della protezione dei dati notifica annualmente alla Commissione le sanzioni amministrative pecuniarie da esso inflitte a norma del presente articolo e qualsiasi controversia o procedimento giudiziario che ha avviato.

Articolo 101

Sanzioni pecuniarie per i fornitori di modelli di IA per finalità generali

1. La Commissione può infliggere ai fornitori di modelli di IA per finalità generali sanzioni pecuniarie non superiori al 3 % del fatturato mondiale annuo totale dell'esercizio precedente o a 15 000 000 EUR, se superiore, ove essa rilevi che il fornitore, intenzionalmente o per negligenza:
 - a) ha violato le pertinenti disposizioni del presente regolamento;
 - b) non ha ottemperato a una richiesta di documento o di informazioni a norma dell'articolo 91 o ha fornito informazioni inesatte, incomplete o fuorvianti;

- c) non ha ottemperato a una misura richiesta a norma dell'articolo 93;
- d) non ha messo a disposizione della Commissione l'accesso al modello di IA per finalità generali o al modello di IA per finalità generali con rischio sistemico al fine di effettuare una valutazione a norma dell'articolo 92.

Nel determinare l'importo della sanzione pecuniaria o della penalità di mora, si tengono in considerazione la natura, la gravità e la durata della violazione, tenendo debitamente conto dei principi di proporzionalità e di adeguatezza. La Commissione tiene conto anche degli impegni assunti in conformità dell'articolo 93, paragrafo 3, o assunti nei pertinenti codici di condotta in conformità dell'articolo 56.

- 2. Prima di adottare la decisione a norma del paragrafo 1, la Commissione comunica le sue constatazioni preliminari al fornitore del modello di IA per finalità generali o del modello di IA e gli dà l'opportunità di essere ascoltato.
- 3. Le sanzioni pecuniarie inflitte in conformità del presente articolo sono effettive, proporzionate e dissuasive.
- 4. Le informazioni in merito alle sanzioni pecuniarie inflitte a norma del presente articolo sono altresì comunicate al consiglio per l'IA, se del caso.
- 5. La Corte di giustizia dell'Unione europea ha competenza giurisdizionale anche di merito per esaminare le decisioni mediante le quali la Commissione ha fissato una sanzione pecuniaria a norma del presente articolo. Essa può estinguere, ridurre o aumentare la sanzione pecuniaria inflitta.

6. La Commissione adotta atti di esecuzione contenenti modalità dettagliate per i procedimenti e garanzie procedurali in vista dell'eventuale adozione di decisioni a norma del paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.

Capo XIII

Disposizioni finali

Articolo 102

Modifica del regolamento (CE) n. 300/2008

All'articolo 4, paragrafo 3, del regolamento (CE) n. 300/2008 è aggiunto il comma seguente:

"Nell'adottare misure dettagliate relative alle specifiche tecniche e alle procedure per l'approvazione e l'uso delle attrezzature di sicurezza per quanto concerne i sistemi di intelligenza artificiale ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*,+}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...)."

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 103
Modifica del regolamento (UE) n. 167/2013

All'articolo 17, paragrafo 5, del regolamento (UE) n. 167/2013 è aggiunto il comma seguente:

"Nell'adottare atti delegati a norma del primo comma per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*,+}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 104

Modifica del regolamento (UE) n. 168/2013

All'articolo 22, paragrafo 5, del regolamento (UE) n. 168/2013 è aggiunto il comma seguente:

"Nell'adottare atti delegati a norma del primo comma per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*,+}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 105
Modifica della direttiva 2014/90/UE

All'articolo 8 della direttiva 2014/90/UE è aggiunto il paragrafo seguente:

- "5. Per i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*,+}, nello svolgimento delle sue attività a norma del paragrafo 1 e nell'adottare specifiche tecniche e norme di prova conformemente ai paragrafi 2 e 3, la Commissione tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 106
Modifica della direttiva (UE) 2016/797

All'articolo 5 della direttiva (UE) 2016/797 è aggiunto il paragrafo seguente:

"12. Nell'adottare atti delegati a norma del paragrafo 1 e atti di esecuzione a norma del paragrafo 11 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*,+}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 107
Modifica del regolamento (UE) 2018/858

All'articolo 5 del regolamento (UE) 2018/858 è aggiunto il paragrafo seguente:

- "4. "Nell'adottare atti delegati a norma del paragrafo 3 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*,+}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 108
Modifiche del regolamento (UE) 2018/1139

Il regolamento (UE) 2018/1139 è così modificato:

1) all'articolo 17 è aggiunto il paragrafo seguente:

"3. Fatto salvo il paragrafo 2, nell'adottare atti di esecuzione a norma del paragrafo 1 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio ^{*,+}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento(UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).";

2) all'articolo 19 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... ⁺⁺, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.";

⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

⁺⁺ GU: inserire il numero del presente regolamento (2021/0106 (COD)).

3) all'articolo 43 è aggiunto il paragrafo seguente:

"4. Nell'adottare atti di esecuzione a norma del paragrafo 1 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/...⁺, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.";

4) all'articolo 47 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/...⁺, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.";

5) all'articolo 57 è aggiunto il comma seguente:

"Nell'adottare tali atti di esecuzione per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/...⁺, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.";

6) all'articolo 58 è aggiunto il paragrafo seguente:

"3. Nell'adottare atti delegati a norma dei paragrafi 1 e 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/...⁺, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.".

⁺ GU: inserire il numero del presente regolamento (2021/0106 (COD)).

⁺ GU: inserire il numero del presente regolamento (2021/0106 (COD)).

Articolo 109
Modifica del regolamento (UE) 2019/2144

All'articolo 11 del regolamento (UE) 2019/2144 è aggiunto il paragrafo seguente:

- "3. "Nell'adottare atti di esecuzione a norma del paragrafo 2 per quanto concerne i sistemi di intelligenza artificiale che sono componenti di sicurezza ai sensi del regolamento (UE) 2024/... del Parlamento europeo e del Consiglio^{*++}, si tiene conto dei requisiti di cui al capo III, sezione 2, di tale regolamento.

* Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio, del ..., che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

⁺⁺ GU: inserire nel testo il numero del presente regolamento (2021/0106(COD)) e completare la corrispondente nota a piè di pagina.

Articolo 110
Modifica della direttiva (UE) 2020/1828

All'allegato I della direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio¹⁷⁴ è aggiunto il punto seguente:

"68) Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio del ...⁺ che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (GU L, ..., ELI: ...).".

Articolo 111
Sistemi di IA già immessi sul mercato o messi in servizio
e modelli di IA per finalità generali già immessi sul mercato

1. Fatta salva l'applicazione dell'articolo 5 di cui all'articolo 113, paragrafo 3, lettera a), i sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'allegato X che sono stati immessi sul mercato o messi in servizio prima del ... [36 mesi dalla data di entrata in vigore del presente regolamento] sono resi conformi al presente regolamento entro il 31 dicembre 2030.

¹⁷⁴ Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, relativa alle azioni rappresentative a tutela degli interessi collettivi dei consumatori e che abroga la direttiva 2009/22/CE (GU L 409 del 4.12.2020, pag. 1).

⁺ GU: Inserire nel testo la data e il numero del presente regolamento (2021/0106(COD)).

Si tiene conto dei requisiti di cui al presente regolamento nella valutazione di ciascun sistema IT su larga scala istituito dagli atti giuridici elencati nell'allegato X da effettuare come previsto in tali atti giuridici e ove tali atti giuridici siano sostituiti o modificati.

2. Fatta salva l'applicazione dell'articolo 5 di cui all'articolo 113, paragrafo 3, lettera a), il presente regolamento si applica agli operatori dei sistemi di IA ad alto rischio, diversi dai sistemi di cui al paragrafo 1 del presente articolo, che sono stati immessi sul mercato o messi in servizio prima del ... [24 mesi dalla data di entrata in vigore del presente regolamento], solo se, a decorrere da tale data, tali sistemi sono soggetti a modifiche significative della loro progettazione. In ogni caso, i fornitori e deployers di sistemi di IA ad alto rischio destinati a essere utilizzati dalle autorità pubbliche adottano le misure necessarie per conformarsi ai requisiti e agli obblighi del presente regolamento entro il ... [sei anni dalla data di entrata in vigore del presente regolamento].
3. I fornitori di modelli di IA per finalità generali che sono stati immessi sul mercato prima del ... [12 mesi dalla data di entrata in vigore del presente regolamento] adottano le misure necessarie per conformarsi agli obblighi di cui al presente regolamento entro ... [36 mesi dalla data di entrata in vigore del presente regolamento].

Articolo 112
Valutazione e riesame

1. La Commissione valuta la necessità di modificare l'elenco stabilito nell'allegato III e l'elenco di pratiche di IA vietate di cui all'articolo 5 una volta all'anno dopo l'entrata in vigore del presente regolamento e fino al termine del periodo della delega di potere di cui all'articolo 97. La Commissione trasmette i risultati della valutazione al Parlamento europeo e al Consiglio.
2. Entro ... [quattro anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni quattro anni, la Commissione valuta e riferisce al Parlamento europeo e al Consiglio in merito a quanto segue:
 - a) la necessità di modifiche che amplino le rubriche settoriali esistenti o ne aggiungano di nuove all'allegato III;
 - b) modifiche dell'elenco dei sistemi di IA che richiedono ulteriori misure di trasparenza di cui all'articolo 50;
 - c) modifiche volte a migliorare l'efficacia del sistema di supervisione e di governance.

3. Entro ... [cinque anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento. La relazione include una valutazione in merito alla struttura di esecuzione e all'eventuale necessità di un'agenzia dell'Unione che ponga rimedio alle carenze individuate. Sulla base dei risultati, la relazione è corredata, se del caso, di una proposta di modifica del presente regolamento. Le relazioni sono rese pubbliche.
4. Le relazioni di cui al paragrafo 2 dedicano particolare attenzione agli aspetti seguenti:
- a) lo stato delle risorse finanziarie, tecniche e umane necessarie alle autorità nazionali competenti per lo svolgimento efficace dei compiti loro assegnati a norma del presente regolamento;
 - b) lo stato delle sanzioni, in particolare delle sanzioni amministrative pecuniarie di cui all'articolo 99, paragrafo 1, applicate dagli Stati membri in caso di violazione del presente regolamento;
 - c) le norme armonizzate adottate e le specifiche comuni elaborate a sostegno del presente regolamento;
 - d) il numero di imprese che entrano sul mercato dopo l'entrata in vigore del presente regolamento e quante di esse sono PMI.

5. Entro ... [quattro anni dalla data di entrata in vigore del presente regolamento], la Commissione valuta il funzionamento dell'ufficio per l'IA, se all'ufficio per l'IA siano stati conferiti poteri e competenze adeguati per svolgere i suoi compiti e se sia pertinente e necessario per la corretta attuazione ed esecuzione del presente regolamento potenziare l'ufficio per l'IA e le sue competenze di esecuzione e aumentarne le risorse. La Commissione trasmette una relazione sulla valutazione di tale ufficio per l'IA al Parlamento europeo e al Consiglio.
6. Entro ... [quattro anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni quattro anni, la Commissione presenta una relazione sull'esame dei progressi compiuti riguardo allo sviluppo di prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico di modelli di IA per finalità generali e valuta la necessità di ulteriori misure o azioni, comprese misure o azioni vincolanti. La relazione è presentata al Parlamento europeo e al Consiglio ed è resa pubblica.
7. Entro ... [quattro anni dalla data di entrata in vigore del presente regolamento] e successivamente ogni tre anni la Commissione valuta l'impatto e l'efficacia dei codici di condotta volontari per la promozione dell'applicazione dei requisiti di cui al capo III, sezione 2, per i sistemi di IA diversi dai sistemi di IA ad alto rischio ed eventualmente di altri requisiti supplementari per i sistemi di IA diversi dai sistemi di IA ad alto rischio, anche per quanto riguarda la sostenibilità ambientale.
8. Ai fini dei paragrafi da 1 a 7, il consiglio per l'IA, gli Stati membri e le autorità nazionali competenti forniscono alla Commissione informazioni su sua richiesta e senza indebito ritardo.

9. Nello svolgere le valutazioni e i riesami di cui ai paragrafi da 1 a 7, la Commissione tiene conto delle posizioni e delle conclusioni del consiglio per l'IA, del Parlamento europeo e del Consiglio, nonché di altri organismi o fonti pertinenti.
10. Se necessario, la Commissione presenta opportune proposte di modifica del presente regolamento tenendo conto, in particolare, degli sviluppi delle tecnologie e dell'effetto dei sistemi di IA sulla salute, sulla sicurezza e sui diritti fondamentali, nonché alla luce dei progressi della società dell'informazione.
11. Per orientare le valutazioni e i riesami di cui ai paragrafi da 1 a 7, l'Ufficio per l'IA si impegna a sviluppare una metodologia obiettiva e partecipativa per la valutazione dei livelli di rischio basata sui criteri definiti negli articoli pertinenti e l'inclusione di nuovi sistemi:
- a) nell'elenco stabilito nell'allegato III, compreso l'ampliamento delle rubriche settoriali esistenti o l'aggiunta di nuove rubriche settoriali in tale allegato;
 - b) nell'elenco delle pratiche vietate stabilite all'articolo 5; e
 - c) nell'elenco dei sistemi di IA che richiedono ulteriori misure di trasparenza a norma dell'articolo 50.
12. Eventuali modifiche al presente regolamento a norma del paragrafo 10, o i pertinenti atti delegati o di esecuzione, che riguardano la normativa settoriale di armonizzazione dell'Unione elencata nell'allegato I, sezione B, tengono conto delle specificità normative di ciascun settore e dei vigenti meccanismi di governance, valutazione della conformità ed esecuzione e delle autorità da essi stabilite.

13. Entro ... [sette anni dalla data di entrata in vigore del presente regolamento], la Commissione effettua una valutazione dell'esecuzione del presente regolamento e riferisce in merito al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo, tenendo conto dei primi anni di applicazione del presente regolamento. Sulla base dei risultati, la relazione è accompagnata, se del caso, da una proposta di modifica del presente regolamento in relazione alla struttura di esecuzione e alla necessità di un'agenzia dell'Unione che ponga rimedio alle carenze individuate.

Articolo 113

Entrata in vigore e applicazione

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Si applica a decorrere dal ... [24 mesi dalla data di entrata in vigore del presente regolamento].

Tuttavia:

- a) I capi I e II si applicano a decorrere dal ... [sei mesi dalla data di entrata in vigore del presente regolamento];
- b) Il capo III, sezione 4, il capo V, il capo VII, il capo XII e l'articolo 78 si applicano a decorrere dal ... [12 mesi dalla data di entrata in vigore del presente regolamento], ad eccezione dell'articolo 101;

- c) L'articolo 6, paragrafo 1, e i corrispondenti obblighi di cui al presente regolamento si applicano a decorrere dal... [36 mesi dalla data di entrata in vigore del presente regolamento].

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles,

Per il Parlamento europeo

La presidente

Per il Consiglio

Il presidente

ALLEGATO I

Elenco della normativa di armonizzazione dell'Unione

Sezione A. Elenco della normativa di armonizzazione dell'Unione in base al nuovo quadro legislativo

1. Direttiva 2006/42/CE del Parlamento europeo e del Consiglio, del 17 maggio 2006, relativa alle macchine e che modifica la direttiva 95/16/CE (GU L 157 del 9.6.2006, pag. 24) [abrogata dal regolamento sui prodotti macchina];
2. direttiva 2009/48/CE del Parlamento europeo e del Consiglio, del 18 giugno 2009, sulla sicurezza dei giocattoli (GU L 170 del 30.6.2009, pag. 1);
3. direttiva 2013/53/UE del Parlamento europeo e del Consiglio, del 20 novembre 2013, relativa alle imbarcazioni da diporto e alle moto d'acqua e che abroga la direttiva 94/25/CE (GU L 354 del 28.12.2013, pag. 90);
4. direttiva 2014/33/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, per l'armonizzazione delle legislazioni degli Stati membri relative agli ascensori e ai componenti di sicurezza per ascensori (GU L 96 del 29.3.2014, pag. 251);
5. direttiva 2014/34/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative agli apparecchi e sistemi di protezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva (GU L 96 del 29.3.2014, pag. 309);

6. direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE (GU L 153 del 22.5.2014, pag. 62);
7. direttiva 2014/68/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di attrezzature a pressione (GU L 189 del 27.6.2014, pag. 164);
8. regolamento (UE) 2016/424 del Parlamento europeo e del Consiglio, del 9 marzo 2016, relativo agli impianti a fune e che abroga la direttiva 2000/9/CE (GU L 81 del 31.3.2016, pag. 1);
9. regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio (GU L 81 del 31.3.2016, pag. 51);
10. regolamento (UE) 2016/426 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sugli apparecchi che bruciano carburanti gassosi e che abroga la direttiva 2009/142/CE (GU L 81 del 31.3.2016, pag. 99);
11. regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio (GU L 117 del 5.5.2017, pag. 1);

12. regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici *in vitro* e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, pag. 176).

Sezione B – Elenco di altre normative di armonizzazione dell'Unione

13. Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio, dell'11 marzo 2008, che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002 (GU L 97 del 9.4.2008, pag. 72);
14. regolamento (UE) n. 168/2013 del Parlamento europeo e del Consiglio, del 15 gennaio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore a due o tre ruote e dei quadricicli (GU L 60 del 2.3.2013, pag. 52);
15. regolamento (UE) n. 167/2013 del Parlamento europeo e del Consiglio, del 5 febbraio 2013, relativo all'omologazione e alla vigilanza del mercato dei veicoli agricoli e forestali (GU L 60 del 2.3.2013, pag. 1);
16. direttiva 2014/90/UE del Parlamento europeo e del Consiglio, del 23 luglio 2014, sull'equipaggiamento marittimo e che abroga la direttiva 96/98/CE del Consiglio (GU L 257 del 28.8.2014, pag. 146);
17. direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, relativa all'interoperabilità del sistema ferroviario dell'Unione europea (GU L 138 del 26.5.2016, pag. 44);

18. regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio, del 30 maggio 2018, relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE (GU L 151 del 14.6.2018, pag. 1);
19. regolamento (UE) 2019/2144 del Parlamento europeo e del Consiglio, del 27 novembre 2019, relativo ai requisiti di omologazione dei veicoli a motore e dei loro rimorchi, nonché di sistemi, componenti ed entità tecniche destinati a tali veicoli, per quanto riguarda la loro sicurezza generale e la protezione degli occupanti dei veicoli e degli altri utenti vulnerabili della strada, che modifica il regolamento (UE) 2018/858 del Parlamento europeo e del Consiglio e abroga i regolamenti (CE) n. 78/2009, (CE) n. 79/2009 e (CE) n. 661/2009 del Parlamento europeo e del Consiglio e i regolamenti (CE) n. 631/2009, (UE) n. 406/2010, (UE) n. 672/2010, (UE) n. 1003/2010, (UE) n. 1005/2010, (UE) n. 1008/2010, (UE) n. 1009/2010, (UE) n. 19/2011, (UE) n. 109/2011, (UE) n. 458/2011, (UE) n. 65/2012, (UE) n. 130/2012, (UE) n. 347/2012, (UE) n. 351/2012, (UE) n. 1230/2012 e (UE) 2015/166 della Commissione (GU L 325 del 16.12.2019, pag. 1);

20. regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio, del 4 luglio 2018, recante norme comuni nel settore dell'aviazione civile, che istituisce un'Agenzia dell'Unione europea per la sicurezza aerea e che modifica i regolamenti (CE) n. 2111/2005, (CE) n. 1008/2008, (UE) n. 996/2010, (UE) n. 376/2014 e le direttive 2014/30/UE e 2014/53/UE del Parlamento europeo e del Consiglio, e abroga i regolamenti (CE) n. 552/2004 e (CE) n. 216/2008 del Parlamento europeo e del Consiglio e il regolamento (CEE) n. 3922/91 del Consiglio (GU L 212 del 22.8.2018, pag. 1), nella misura in cui si tratta della progettazione, della produzione e dell'immissione sul mercato degli aeromobili di cui all'articolo 2, paragrafo 1, lettere a) e b), relativamente agli aeromobili senza equipaggio e ai loro motori, eliche, parti e dispositivi di controllo remoto.
-

ALLEGATO II

Elenco dei reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii)

Reati di cui all'articolo 5, paragrafo 1, primo comma, lettera h), punto iii):

- terrorismo,
- tratta di esseri umani,
- sfruttamento sessuale di minori e pornografia minorile,
- traffico illecito di stupefacenti o sostanze psicotrope,
- traffico illecito di armi, munizioni ed esplosivi,
- omicidio volontario, lesioni gravi,
- traffico illecito di organi e tessuti umani,
- traffico illecito di materie nucleari e radioattive,
- sequestro, detenzione illegale e presa di ostaggi,
- reati che rientrano nella competenza giurisdizionale della Corte penale internazionale,
- illecita cattura di aeromobile o nave,

- violenza sessuale,
 - reato ambientale,
 - rapina organizzata o a mano armata,
 - sabotaggio,
 - partecipazione a un'organizzazione criminale coinvolta in uno o più dei reati elencati sopra.
-

ALLEGATO III

Sistemi di IA ad alto rischio di cui all'articolo 6, paragrafo 2

I sistemi di IA ad alto rischio a norma dell'articolo 6, paragrafo 2, sono i sistemi di IA elencati in uno dei settori indicati di seguito.

1. Biometria, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

a) i sistemi di identificazione biometrica remota.

Non vi rientrano i sistemi di IA destinati a essere utilizzati per la verifica biometrica la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere;

b) i sistemi di IA destinati a essere utilizzati per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti basati sulla deduzione di tali attributi o caratteristiche;

c) i sistemi di IA destinati a essere utilizzati per il riconoscimento delle emozioni.

2. Infrastrutture critiche: i sistemi di IA destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità.

3. Istruzione e formazione professionale:

- a) i sistemi di IA destinati a essere utilizzati per determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli;
- b) i sistemi di IA destinati a essere utilizzati per valutare i risultati dell'apprendimento, anche nei casi in cui tali risultati sono utilizzati per orientare il processo di apprendimento di persone fisiche in istituti di istruzione o formazione professionale a tutti i livelli;
- c) i sistemi di IA destinati a essere utilizzati per valutare il livello di istruzione adeguato che una persona riceverà o a cui potrà accedere, nel contesto o all'interno di istituti di istruzione o formazione professionale a tutti i livelli;
- d) i sistemi di IA destinati a essere utilizzati per monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale a tutti i livelli.

4. Occupazione, gestione dei lavoratori e accesso al lavoro autonomo:

- a) i sistemi di IA destinati a essere utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati;

- b) i sistemi di IA destinati a essere utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro.

5. Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi:

- a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;
- b) i sistemi di IA destinati a essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito, a eccezione dei sistemi di IA utilizzati allo scopo di individuare frodi finanziarie;
- c) i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie;
- d) i sistemi di IA destinati a essere utilizzati per valutare e classificare le chiamate di emergenza effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco e assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza;

6. Attività di contrasto, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:
- a) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto o per loro conto, per determinare il rischio per una persona fisica di diventare vittima di reati;
 - b) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, come poligrafi e strumenti analoghi;
 - c) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati;
 - d) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per determinare il rischio di commissione del reato o di recidiva in relazione a una persona fisica non solo sulla base della profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 o per valutare i tratti e le caratteristiche della personalità o il comportamento criminale pregresso di persone fisiche o gruppi;

- e) i sistemi di IA destinati a essere utilizzati dalle autorità di contrasto o per loro conto, oppure da istituzioni, organi e organismi dell'Unione a sostegno delle autorità di contrasto, per effettuare la profilazione delle persone fisiche di cui all'articolo 3, paragrafo 4, della direttiva (UE) 2016/680 nel corso dell'indagine, dell'accertamento e del perseguimento di reati.

7. Migrazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso:

- a) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti, o per loro conto, o da istituzioni, organi e organismi dell'Unione, come poligrafi o strumenti analoghi;
- b) i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per valutare un rischio (compresi un rischio per la sicurezza, un rischio di migrazione irregolare o un rischio per la salute) posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro;
- c) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, oppure da istituzioni, organi e organismi dell'Unione, per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto o di permesso di soggiorno e per i relativi reclami per quanto riguarda l'ammissibilità delle persone fisiche che richiedono tale status, compresa le valutazioni correlate dell'affidabilità degli elementi probatori;

- d) i sistemi di IA destinati a essere usati dalle autorità pubbliche competenti o per loro conto, o da istituzioni, organi e organismi dell'Unione, nel contesto della migrazione, dell'asilo o della gestione del controllo delle frontiere, al fine di individuare, riconoscere o identificare persone fisiche, a eccezione della verifica dei documenti di viaggio.

8. Amministrazione della giustizia e processi democratici:

- a) i sistemi di IA destinati a essere usati da un'autorità giudiziaria o per suo conto per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti e del diritto e nell'applicazione della legge a una serie concreta di fatti, o a essere utilizzati in modo analogo nella risoluzione alternativa delle controversie;
- b) i sistemi di IA destinati a essere utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone fisiche nell'esercizio del loro voto alle elezioni o ai referendum. Sono esclusi i sistemi di IA ai cui output le persone fisiche non sono direttamente esposte, come gli strumenti utilizzati per organizzare, ottimizzare e strutturare le campagne politiche da un punto di vista amministrativo e logistico.

ALLEGATO IV

Documentazione tecnica di cui all'articolo 11, paragrafo 1

La documentazione tecnica di cui all'articolo 11, paragrafo 1, deve includere almeno le seguenti informazioni, a seconda dell'applicabilità al pertinente sistema di IA.

1. Una descrizione generale del sistema di IA comprendente:
 - a) la finalità prevista, il nome del fornitore e la versione del sistema che indichi il suo rapporto con le versioni precedenti;
 - b) il modo in cui il sistema di IA interagisce o può essere utilizzato per interagire con hardware o software, compresi altri sistemi di IA, che non fanno parte del sistema di IA stesso, ove applicabile;
 - c) le versioni dei pertinenti software o firmware e qualsiasi requisito relativo all'aggiornamento della versione;
 - d) la descrizione di tutte le forme in cui il sistema di IA è immesso sul mercato o messo in servizio, quali pacchetti software incorporati nell'hardware, download o API;
 - e) la descrizione dell'hardware su cui è destinato a operare il sistema di IA;
 - f) se il sistema di IA è un componente di prodotti, le fotografie o le illustrazioni che mostrino le caratteristiche esterne, la marcatura e il layout interno di tali prodotti;

- g) una descrizione di base dell'interfaccia utente fornita al deployer;
- h) le istruzioni per l'uso destinate al deployer e una descrizione di base dell'interfaccia utente fornita al deployer, se applicabile.

2. Una descrizione dettagliata degli elementi del sistema di IA e del processo relativo al suo sviluppo, compresi:

- a) i metodi applicati e le azioni eseguite per lo sviluppo del sistema di IA, compresi, ove opportuno, il ricorso a sistemi o strumenti preaddestrati forniti da terzi e il modo in cui sono stati utilizzati, integrati o modificati dal fornitore;
- b) le specifiche di progettazione del sistema, vale a dire la logica generale del sistema di IA e degli algoritmi; le principali scelte di progettazione, comprese le motivazioni e le ipotesi formulate, anche per quanto riguarda le persone o i gruppi di persone sui quali il sistema è destinato a essere utilizzato; le principali scelte di classificazione; gli aspetti che il sistema è progettato per ottimizzare e la pertinenza dei diversi parametri; la descrizione dell'output atteso e della qualità dell'output del sistema; le decisioni in merito a eventuali compromessi posti in essere con riguardo alle soluzioni tecniche adottate per soddisfare i requisiti di cui al capo III, sezione 2;
- c) la descrizione dell'architettura del sistema che spiega in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo; le risorse computazionali utilizzate per sviluppare, addestrare, sottoporre a prova e convalidare il sistema di IA;

- d) ove pertinente, i requisiti in materia di dati mediante schede tecniche che descrivono le metodologie e le tecniche di addestramento e i set di dati di addestramento utilizzati, comprese una descrizione generale di tali set di dati e le informazioni sulla loro origine, sul loro ambito di applicazione e sulle loro principali caratteristiche; le modalità di ottenimento e di selezione dei dati; le procedure di etichettatura, ad esempio per l'apprendimento supervisionato, e le metodologie di pulizia dei dati, ad esempio il rilevamento di valori anomali (outlier);
- e) la valutazione delle misure di sorveglianza umana necessarie in conformità dell'articolo 14, compresa una valutazione delle misure tecniche necessarie per facilitare l'interpretazione degli output dei sistemi di IA da parte dei deployer, in conformità dell'articolo 13, paragrafo 3, lettera d);
- f) ove applicabile, una descrizione dettagliata delle modifiche predeterminate del sistema di IA e delle sue prestazioni, unitamente a tutte le informazioni pertinenti relative alle soluzioni tecniche adottate per garantire la conformità costante del sistema di IA ai requisiti pertinenti di cui al capo III, sezione 2;
- g) le procedure di convalida e di prova utilizzate, comprese le informazioni sui dati di convalida e di prova utilizzati e sulle loro principali caratteristiche; le metriche utilizzate per misurare l'accuratezza, la robustezza e la conformità ad altri requisiti pertinenti di cui al capo III, sezione 2, nonché gli impatti potenzialmente discriminatori; i log delle prove e tutte le relazioni di prova corredate di data e firma delle persone responsabili, anche per quanto riguarda le modifiche predeterminate di cui alla lettera f);
- h) le misure di cibersicurezza poste in essere.

3. Informazioni dettagliate sul monitoraggio, sul funzionamento e sul controllo del sistema di IA, in particolare per quanto riguarda: le sue capacità e limitazioni in termini di prestazioni, compresi i gradi di accuratezza relativi a determinate persone o determinati gruppi di persone sui quali il sistema è destinato a essere utilizzato e il livello di accuratezza complessivo atteso in relazione alla finalità prevista del sistema; i prevedibili risultati indesiderati e fonti di rischio per la salute, la sicurezza e i diritti fondamentali, nonché di rischio di discriminazione in considerazione della finalità prevista del sistema di IA; le misure di sorveglianza umana necessarie in conformità dell'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte dei deployer; le specifiche relative ai dati di input, se del caso.
4. Una descrizione dell'adeguatezza delle metriche di prestazione per il sistema di IA specifico.
5. Una descrizione dettagliata del sistema di gestione dei rischi in conformità dell'articolo 9.
6. Una descrizione delle modifiche pertinenti apportate dal fornitore al sistema durante il suo ciclo di vita.
7. Un elenco delle norme armonizzate applicate integralmente o in parte i cui riferimenti sono stati pubblicati nella *Gazzetta ufficiale dell'Unione europea*; nei casi in cui tali norme armonizzate non sono state applicate, una descrizione dettagliata delle soluzioni adottate per soddisfare i requisiti di cui al capo III, sezione 2, compreso un elenco delle altre norme e specifiche tecniche pertinenti applicate.
8. Una copia della dichiarazione di conformità UE di cui all'articolo 47.
9. Una descrizione dettagliata del sistema predisposto per valutare le prestazioni del sistema di IA nella fase successiva all'immissione sul mercato in conformità dell'articolo 72, compreso il piano di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72, paragrafo 3.

ALLEGATO V

Dichiarazione di conformità UE

La dichiarazione di conformità UE di cui all'articolo 47 deve contenere tutte le informazioni seguenti:

1. il nome e il tipo del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;
2. il nome e l'indirizzo del fornitore o, ove applicabile, del suo rappresentante autorizzato;
3. un'attestazione secondo cui la dichiarazione di conformità UE di cui all'articolo 47 è rilasciata sotto la responsabilità esclusiva del fornitore;
4. un'attestazione secondo cui il sistema di IA è conforme al presente regolamento e, ove applicabile, a qualsiasi altra disposizione pertinente del diritto dell'Unione che preveda il rilascio di una dichiarazione di conformità UE di cui all'articolo 47;
5. se un sistema di IA comporta il trattamento di dati personali, una dichiarazione attestante che tale sistema di IA è conforme ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680;
6. i riferimenti alle pertinenti norme armonizzate utilizzate o a qualsiasi altra specifica comune in relazione alla quale è dichiarata la conformità;

7. ove applicabile, il nome e il numero di identificazione dell'organismo notificato, una descrizione della procedura di valutazione della conformità applicata e l'identificazione del certificato rilasciato;
 8. il luogo e la data di rilascio della dichiarazione, il nome e la funzione della persona che firma la dichiarazione nonché un'indicazione della persona a nome o per conto della quale ha firmato, e la firma.
-

ALLEGATO VI

Procedura di valutazione della conformità basata sul controllo interno

1. La procedura di valutazione della conformità basata sul controllo interno è la procedura di valutazione della conformità basata sui punti 2, 3 e 4.
 2. Il fornitore verifica la conformità del sistema di gestione della qualità istituito ai requisiti di cui all'articolo 17.
 3. Il fornitore esamina le informazioni contenute nella documentazione tecnica al fine di valutare la conformità del sistema di IA ai pertinenti requisiti essenziali di cui al capo III, sezione 2.
 4. Il fornitore verifica inoltre che il processo di progettazione e sviluppo del sistema di IA e il monitoraggio successivo alla sua immissione sul mercato di cui all'articolo 72 siano coerenti con la documentazione tecnica.
-

ALLEGATO VII

Conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica

1. Introduzione

La conformità basata su una valutazione del sistema di gestione della qualità e su una valutazione della documentazione tecnica scaturisce dalla procedura di valutazione della conformità di cui ai punti da 2 a 5.

2. Aspetti generali

Il sistema di gestione della qualità approvato per la progettazione, lo sviluppo e la prova dei sistemi di IA a norma dell'articolo 17 deve essere esaminato conformemente al punto 3 e deve essere soggetto alla vigilanza di cui al punto 5. La documentazione tecnica del sistema di IA deve essere esaminata conformemente al punto 4.

3. Sistema di gestione della qualità

3.1. La domanda presentata dal fornitore deve comprendere:

- a) il nome e l'indirizzo del fornitore e, nel caso in cui la domanda sia presentata da un rappresentante autorizzato, anche il nome e l'indirizzo di quest'ultimo;
- b) l'elenco dei sistemi di IA cui si applica lo stesso sistema di gestione della qualità;
- c) la documentazione tecnica di ciascuno dei sistemi di IA cui si applica lo stesso sistema di gestione della qualità;

- d) la documentazione relativa al sistema di gestione della qualità che deve contemplare tutti gli aspetti elencati all'articolo 17;
- e) una descrizione delle procedure vigenti per garantire che il sistema di gestione della qualità rimanga adeguato ed efficace;
- f) una dichiarazione scritta attestante che la stessa domanda non è stata presentata a nessun altro organismo notificato.

3.2. Il sistema di gestione della qualità deve essere valutato dall'organismo notificato, che deve stabilire se soddisfa i requisiti di cui all'articolo 17.

La decisione deve essere notificata al fornitore o al suo rappresentante autorizzato.

Tale notifica deve indicare le conclusioni della valutazione del sistema di gestione della qualità e la decisione di valutazione motivata.

3.3. Il sistema di gestione della qualità approvato deve continuare a essere attuato e mantenuto dal fornitore in modo da rimanere adeguato ed efficiente.

3.4. Il fornitore deve portare all'attenzione dell'organismo notificato qualsiasi modifica prevista del sistema di gestione della qualità approvato o dell'elenco dei sistemi di IA cui si applica tale sistema.

Le modifiche proposte devono essere esaminate dall'organismo notificato, che deve decidere se il sistema di gestione della qualità modificato continua a soddisfare i requisiti di cui al punto 3.2 o se è necessaria una nuova valutazione.

L'organismo notificato deve notificare al fornitore la propria decisione. Tale notifica deve indicare le conclusioni dell'esame e la decisione di valutazione motivata.

4. Controllo della documentazione tecnica.
 - 4.1. Oltre alla domanda di cui al punto 3, il fornitore deve presentare una domanda a un organismo notificato di propria scelta per la valutazione della documentazione tecnica relativa al sistema di IA che il fornitore intende immettere sul mercato o mettere in servizio e cui si applica il sistema di gestione della qualità di cui al punto 3.
 - 4.2. La domanda deve comprendere:
 - a) il nome e l'indirizzo del fornitore;
 - b) una dichiarazione scritta attestante che la stessa domanda non è stata presentata a nessun altro organismo notificato;
 - c) la documentazione tecnica di cui all'allegato IV.
 - 4.3. La documentazione tecnica deve essere esaminata dall'organismo notificato. Se del caso e nei limiti di quanto necessario per lo svolgimento dei suoi compiti, all'organismo notificato deve essere concesso pieno accesso ai set di dati di addestramento, convalida e prova utilizzati, anche, ove opportuno e fatte salve le garanzie di sicurezza, attraverso API o altri mezzi e strumenti tecnici pertinenti che consentano l'accesso remoto.

- 4.4. Nell'esaminare la documentazione tecnica, l'organismo notificato può chiedere al fornitore di presentare elementi probatori supplementari o di eseguire ulteriori prove per consentire una corretta valutazione della conformità del sistema di IA ai requisiti di cui al capo III, sezione 2. Qualora non sia soddisfatto delle prove effettuate dal fornitore, l'organismo notificato stesso deve effettuare prove adeguate, a seconda dei casi.
- 4.5. Ove necessario per valutare la conformità del sistema di IA ad alto rischio ai requisiti di cui al capo III, sezione 2, dopo che tutti gli altri mezzi ragionevoli per verificare la conformità sono stati esauriti e si sono rivelati insufficienti, e su richiesta motivata, anche all'organismo notificato deve essere concesso l'accesso ai modelli di addestramento e addestrati del sistema di IA, compresi i relativi parametri. Tale accesso è soggetto al vigente diritto dell'Unione in materia di protezione della proprietà intellettuale e dei segreti commerciali.
- 4.6. La decisione dell'organismo notificato deve essere notificata al fornitore o al suo rappresentante autorizzato. Tale notifica deve indicare le conclusioni della valutazione della documentazione tecnica e la decisione di valutazione motivata.

Se il sistema di IA è conforme ai requisiti di cui al capo III, sezione 2, l'organismo notificato deve rilasciare un certificato di valutazione della documentazione tecnica dell'Unione. Tale certificato deve indicare il nome e l'indirizzo del fornitore, le conclusioni dell'esame, le eventuali condizioni di validità e i dati necessari per identificare il sistema di IA.

Il certificato e i suoi allegati devono contenere tutte le informazioni pertinenti per consentire la valutazione della conformità del sistema di IA e il controllo del sistema di IA durante l'uso, ove applicabile.

Se il sistema di IA non è conforme ai requisiti di cui al capo III, sezione 2, l'organismo notificato deve rifiutare il rilascio di un certificato di valutazione della documentazione tecnica dell'Unione e deve informare in merito il richiedente, motivando dettagliatamente il suo rifiuto.

Se il sistema di IA non soddisfa il requisito relativo ai dati utilizzati per l'addestramento, sarà necessario addestrare nuovamente il sistema di IA prima di presentare domanda per una nuova valutazione della conformità. In tal caso, la decisione di valutazione motivata dell'organismo notificato che rifiuta il rilascio del certificato di valutazione della documentazione tecnica dell'Unione contiene considerazioni specifiche sui dati di qualità utilizzati per addestrare il sistema di IA, in particolare sui motivi della non conformità.

- 4.7. Qualsiasi modifica del sistema di IA che potrebbe incidere sulla conformità ai requisiti o sulla finalità prevista dello stesso deve essere valutata dall'organismo notificato che ha rilasciato il certificato di valutazione della documentazione tecnica dell'Unione. Il fornitore deve informare tale organismo notificato quando intende introdurre una delle modifiche di cui sopra o quando viene altrimenti a conoscenza del verificarsi di tali modifiche. Le modifiche previste devono essere valutate dall'organismo notificato, che deve decidere se esse rendono necessaria una nuova valutazione della conformità a norma dell'articolo 43, paragrafo 4, o se possono essere gestite tramite un supplemento del certificato di valutazione della documentazione tecnica dell'Unione. In quest'ultimo caso, l'organismo notificato deve valutare le modifiche, notificare al fornitore la propria decisione e, in caso di approvazione delle modifiche, rilasciare a quest'ultimo un supplemento del certificato di valutazione della documentazione tecnica dell'Unione.

5. Vigilanza del sistema di gestione della qualità approvato.
- 5.1. La finalità della vigilanza a cura dell'organismo notificato di cui al punto 3 è garantire che il fornitore sia conforme ai termini e alle condizioni del sistema di gestione della qualità approvato.
- 5.2. Ai fini della valutazione, il fornitore deve consentire all'organismo notificato di accedere ai locali in cui hanno luogo la progettazione, lo sviluppo e le prove dei sistemi di IA. Il fornitore deve inoltre condividere con l'organismo notificato tutte le informazioni necessarie.
- 5.3. L'organismo notificato deve eseguire audit periodici per assicurarsi che il fornitore mantenga e applichi il sistema di gestione della qualità e deve trasmettere al fornitore una relazione di audit. Nel contesto di tali audit, l'organismo notificato può effettuare prove supplementari dei sistemi di IA per i quali è stato rilasciato un certificato di valutazione della documentazione tecnica dell'Unione.
-

ALLEGATO VIII

Informazioni da presentare all'atto della registrazione
di sistemi di IA ad alto rischio in conformità dell'articolo 49

Sezione A - Informazioni che i fornitori di sistemi di IA ad alto rischio devono presentare in
conformità dell'articolo 49, paragrafo 1

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA ad alto rischio che devono essere registrati a norma dell'articolo 49, paragrafo 1:

1. il nome, l'indirizzo e i dati di contatto del fornitore;
2. se le informazioni sono trasmesse da un'altra persona per conto del fornitore: il nome, l'indirizzo e i dati di contatto di tale persona;
3. il nome, l'indirizzo e i dati di contatto del rappresentante autorizzato, ove applicabile;
4. la denominazione commerciale del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;
5. la descrizione della finalità prevista del sistema di IA e dei componenti e delle funzioni supportati da tale sistema di IA;
6. una descrizione di base concisa delle informazioni utilizzate dal sistema (dati, input) e della sua logica operativa;

7. lo status del sistema di IA (sul mercato, o in servizio; non più immesso sul mercato/in servizio, richiamato);
8. il tipo, il numero e la data di scadenza del certificato rilasciato dall'organismo notificato e il nome o il numero di identificazione di tale organismo notificato, ove applicabile;
9. una copia scannerizzata del certificato di cui al punto 8, ove applicabile;
10. eventuali Stati membri dell'Unione in cui il sistema di IA è stato immesso sul mercato, messo in servizio o reso disponibile;
11. una copia della dichiarazione di conformità UE di cui all'articolo 47;
12. le istruzioni per l'uso in formato elettronico; questa informazione non deve essere fornita per i sistemi di IA ad alto rischio nei settori delle attività di contrasto o della migrazione, dell'asilo e della gestione del controllo delle frontiere di cui all'allegato III, punti 1, 6 e 7;
13. un indirizzo internet per ulteriori informazioni (facoltativo).

Sezione B - Informazioni che i fornitori di sistemi di IA ad alto rischio devono presentare
in conformità dell'articolo 49, paragrafo 2

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA che devono essere registrati a norma dell'articolo 49, paragrafo 2:

1. il nome, l'indirizzo e i dati di contatto del fornitore;
2. se le informazioni sono trasmesse da un'altra persona per conto del fornitore: il nome, l'indirizzo e i dati di contatto di tale persona;
3. il nome, l'indirizzo e i dati di contatto del rappresentante autorizzato, ove applicabile;
4. la denominazione commerciale del sistema di IA e qualsiasi ulteriore riferimento inequivocabile che ne consenta l'identificazione e la tracciabilità;
5. la descrizione della finalità prevista del sistema di IA;
6. la o le condizioni di cui all'articolo 6, paragrafo 3, sulla base delle quali il sistema di IA non è ritenuto ad alto rischio;
7. una breve sintesi dei motivi per i quali il sistema di IA non è ritenuto ad alto rischio in applicazione della procedura di cui all'articolo 6, paragrafo 3;
8. lo status del sistema di IA (sul mercato, o in servizio; non più immesso sul mercato/in servizio, richiamato);
9. eventuali Stati membri dell'Unione in cui il sistema di IA è stato immesso sul mercato, messo in servizio o reso disponibile.

Sezione C - Informazioni che i deployer di sistemi di IA ad alto rischio devono presentare in conformità dell'articolo 49, paragrafo 3

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione ai sistemi di IA ad alto rischio che devono essere registrati a norma dell'articolo 49:

1. il nome, l'indirizzo e i dati di contatto del deployer;
2. il nome, l'indirizzo e i dati di contatto della persona che fornisce informazioni a nome del deployer;
3. l'indirizzo internet dell'inserimento del sistema di IA nella banca dati dell'UE da parte del suo fornitore;
4. una sintesi dei risultati della valutazione d'impatto sui diritti fondamentali effettuata a norma dell'articolo 27;
5. una sintesi della valutazione d'impatto sulla protezione dei dati effettuata ai sensi dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, come specificato all'articolo 26, paragrafo 8, del presente regolamento, ove applicabile.

ALLEGATO IX

Informazioni da presentare all'atto della registrazione dei sistemi di IA ad alto rischio elencati nell'allegato III in relazione alle prove in condizioni reali in conformità dell'articolo 60

Le seguenti informazioni devono essere fornite e successivamente aggiornate in relazione alle prove in condizioni reali che devono essere registrate a norma dell'articolo 60:

1. un numero di identificazione unico a livello dell'Unione della prova in condizioni reali;
2. il nome e i dati di contatto del fornitore o potenziale fornitore e dei deployer coinvolti nella prova in condizioni reali;
3. una breve descrizione del sistema di IA, la sua finalità prevista e altre informazioni necessarie per l'identificazione del sistema;
4. una sintesi delle principali caratteristiche del piano di prova in condizioni reali;
5. informazioni sulla sospensione o sulla cessazione della prova in condizioni reali.

ALLEGATO X

Atti legislativi dell'Unione sui sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia

1. Sistema di informazione Schengen

- a) Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 312 del 7.12.2018, pag. 1).
- b) regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 (GU L 312 del 7.12.2018, pag. 14).
- c) regolamento (UE) 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018, pag. 56).

2. Sistema di informazione visti

- a) Regolamento (UE) 2021/1133 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che modifica i regolamenti (UE) n. 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 e (UE) 2019/818 per quanto riguarda la definizione delle condizioni di accesso agli altri sistemi di informazione dell'UE ai fini del sistema di informazione visti (GU L 248 del 13.7.2021, pag. 1);
- b) regolamento (UE) 2021/1134 del Parlamento europeo e del Consiglio, del 7 luglio 2021, che modifica i regolamenti (CE) n. 767/2008, (CE) n. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (UE) 2019/1896 del Parlamento europeo e del Consiglio e che abroga le decisioni 2004/512/CE e 2008/633/GAI del Consiglio, ai fini della riforma del sistema di informazione visti (GU L 248 del 13.7.2021, pag. 11)

3. Eurodac

Regolamento (UE) 2024/... del Parlamento europeo e del Consiglio che istituisce l'"Eurodac" per il confronto dei dati biometrici ai fini dell'applicazione efficace dei regolamenti (UE) 2024/... e (UE) 2024/... del Parlamento europeo e del Consiglio e della direttiva 2001/55/CE del Consiglio e ai fini dell'identificazione dei cittadini di paesi terzi e apolidi il cui soggiorno è irregolare, e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, che modifica i regolamenti (UE) 2018/1240 e (UE) 2019/818 del Parlamento europeo e del Consiglio e che abroga il regolamento (UE) n. 603/2013 del Parlamento europeo e del Consiglio ⁺.

4. Sistema di ingressi/uscite

Regolamento (UE) 2017/2226 del Parlamento europeo e del Consiglio, del 30 novembre 2017, che istituisce un sistema di ingressi/uscite per la registrazione dei dati di ingresso e di uscita e dei dati relativi al respingimento dei cittadini di paesi terzi che attraversano le frontiere esterne degli Stati membri e che determina le condizioni di accesso al sistema di ingressi/uscite a fini di contrasto e che modifica la Convenzione di applicazione dell'Accordo di Schengen e i regolamenti (CE) n. 767/2008 e (UE) n. 1077/2011 (GU L 327 del 9.12.2017, pag. 20).

⁺ GU: Inserire nel testo il numero del regolamento di cui al documento PE-CONS 15/24 (2016/0132 (COD)) e inserire il numero, la data, il titolo e il riferimento GU di detto regolamento nella nota a piè di pagina.

5. Sistema europeo di informazione e autorizzazione ai viaggi
- a) Regolamento (UE) 2018/1240 del Parlamento europeo e del Consiglio, del 12 settembre 2018, che istituisce un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e che modifica i regolamenti (UE) n. 1077/2011, (UE) n. 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (GU L 236 del 19.9.2018, pag. 1);
 - b) regolamento (UE) 2018/1241 del Parlamento europeo e del Consiglio, del 12 settembre 2018, recante modifica del regolamento (UE) 2016/794 ai fini dell'istituzione di un sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) (GU L 236 del 19.9.2018, pag. 72).
6. Sistema europeo di informazione sui casellari giudiziari riguardo ai cittadini di paesi terzi e apolidi
- Regolamento (UE) 2019/816 del Parlamento europeo e del Consiglio, del 17 aprile 2019, che istituisce un sistema centralizzato per individuare gli Stati membri in possesso di informazioni sulle condanne pronunciate a carico di cittadini di paesi terzi e apolidi (ECRIS-TCN) e integrare il sistema europeo di informazione sui casellari giudiziali, e che modifica il regolamento (UE) 2018/1726 (GU L 135 del 22.5.2019, pag. 1).

7. Interoperabilità

- a) Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019, pag. 27);
 - b) regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019, pag. 85).
-

ALLEGATO XI

Documentazione tecnica di cui all'articolo 53, paragrafo 1, lettera a) — documentazione tecnica per i fornitori di modelli di IA per finalità generali

Sezione 1

Informazioni che devono fornire tutti i fornitori di modelli di IA per finalità generali

La documentazione tecnica di cui all'articolo 53, paragrafo 1, lettera a), deve includere almeno le seguenti informazioni, in funzione della dimensione e del profilo di rischio del modello:

1. Una descrizione generale del modello di IA per finalità generali comprendente:
 - a) i compiti che il modello è destinato a eseguire e il tipo e la natura dei sistemi di IA in cui può essere integrato;
 - b) le politiche di utilizzo accettabili applicabili;
 - c) la data di pubblicazione e i metodi di distribuzione;
 - d) l'architettura e il numero di parametri;
 - e) la modalità (ad esempio testo, immagine) e il formato degli input e degli output;
 - f) la licenza.

2. Una descrizione dettagliata degli elementi del modello di cui al punto 1 e informazioni pertinenti sul processo di sviluppo, compresi gli elementi seguenti:
- a) i mezzi tecnici (ad esempio istruzioni per l'uso, infrastruttura, strumenti) necessari per integrare il modello di IA per finalità generali nei sistemi di IA;
 - b) le specifiche di progettazione del modello e del processo di addestramento, comprese le metodologie e le tecniche di addestramento, le principali scelte progettuali, comprese le motivazioni e le ipotesi formulate; gli aspetti che il modello è progettato per ottimizzare e la pertinenza dei diversi parametri, se del caso;
 - c) informazioni sui dati utilizzati per l'addestramento, la prova e la convalida, se del caso, compresi il tipo e la provenienza dei dati e le metodologie di organizzazione (ad esempio pulizia, filtraggio, ecc.), il numero di punti di dati, la loro portata e le principali caratteristiche; il modo in cui i dati sono stati ottenuti e selezionati e tutte le altre misure per rilevare l'inadeguatezza delle fonti di dati e i metodi per rilevare distorsioni identificabili, se del caso;
 - d) le risorse computazionali utilizzate per addestrare il modello (ad esempio il numero di operazioni in virgola mobile), il tempo di addestramento e altri dettagli pertinenti relativi all'addestramento;
 - e) il consumo energetico noto o stimato del modello.

Per quanto riguarda la lettera e), se il consumo energetico del modello non è noto, il consumo energetico può basarsi su informazioni relative alle risorse computazionali utilizzate.

Sezione 2

Informazioni aggiuntive che devono fornire i fornitori di modelli di IA
per finalità generali con rischio sistemico

1. Una descrizione dettagliata delle strategie di valutazione, compresi i risultati della valutazione, sulla base dei protocolli e degli strumenti di valutazione pubblici disponibili o di altri metodi di valutazione. Le strategie di valutazione comprendono criteri di valutazione, metriche e metodi per l'individuazione delle limitazioni.
 2. Se del caso, una descrizione dettagliata delle misure messe in atto al fine di effettuare il test contraddittorio (adversarial testing) interno e/o esterno (ad esempio, red teaming), adeguamenti dei modelli, compresi l'allineamento e la messa a punto.
 3. Se del caso, una descrizione dettagliata dell'architettura del sistema che spiega in che modo i componenti software si basano l'uno sull'altro o si alimentano reciprocamente e si integrano nel processo complessivo.
-

ALLEGATO XII

- Informazioni sulla trasparenza di cui all'articolo 53, paragrafo 1, lettera b)
- documentazione tecnica per i fornitori di modelli di IA per finalità generali ai fornitori a valle che integrano il modello nel loro sistema di IA

Le informazioni di cui all'articolo 53, paragrafo 1, lettera b), contengono almeno quanto segue:

1. Una descrizione generale del modello di IA per finalità generali comprendente:
 - a) i compiti che il modello è destinato a eseguire e il tipo e la natura dei sistemi di IA in cui può essere integrato;
 - b) le politiche di utilizzo accettabili applicabili;
 - c) la data di pubblicazione e i metodi di distribuzione;
 - d) il modo in cui il modello interagisce o può essere utilizzato per interagire con hardware o software che non fanno parte del modello stesso, ove applicabile;
 - e) le versioni del software pertinente relative all'uso del modello di IA per finalità generali, se del caso;
 - f) l'architettura e il numero di parametri;
 - g) la modalità (ad esempio testo, immagine) e il formato degli input e degli output;
 - h) la licenza per il modello.

2. Una descrizione degli elementi del modello e del processo relativo al suo sviluppo, compresi:
- a) i mezzi tecnici (ad esempio istruzioni per l'uso, infrastruttura, strumenti) necessari per integrare il modello di IA per finalità generali nei sistemi di IA;
 - b) la modalità (ad esempio testo, immagine, ecc.) e il formato degli input e degli output e la loro dimensione massima (ad esempio, lunghezza della finestra contestuale, ecc.);
 - c) informazioni sui dati utilizzati per l'addestramento, la prova e la convalida, se del caso, compresi il tipo e la provenienza dei dati e le metodologie di organizzazione.
-

ALLEGATO XIII

Criteri per la designazione dei modelli di IA per finalità generali con rischio sistemico di cui all'articolo 51

Al fine di determinare se un modello di IA per finalità generali ha capacità o un impatto equivalente a quelli di cui all'articolo 51, paragrafo 1, lettera a), la Commissione tiene conto dei criteri seguenti:

- a) il numero di parametri del modello;
- b) la qualità o la dimensione del set di dati, ad esempio misurata mediante token;
- c) la quantità di calcolo utilizzata per addestrare il modello misurata in operazioni in virgola mobile o indicata da una combinazione di altre variabili quali il costo stimato dell'addestramento, il tempo stimato necessario per l'addestramento o il consumo energetico stimato per l'addestramento;
- d) le modalità di input e output del modello, come da testo a testo (modelli linguistici di grandi dimensioni), da testo a immagine, multimodalità e soglie di punta per determinare le capacità ad alto impatto per ciascuna modalità, nonché il tipo specifico di input e output (ad esempio sequenze biologiche);
- e) i parametri di riferimento e le valutazioni delle capacità del modello, anche tenendo conto del numero di compiti che non richiedono un addestramento aggiuntivo, la capacità di apprendere nuovi compiti distinti, il livello di autonomia e scalabilità e gli strumenti a cui ha accesso;

- f) se il modello ha un alto impatto sul mercato interno in considerazione della sua portata, che viene presunta quando il modello stesso è stato messo a disposizione di almeno 10 000 utenti commerciali registrati stabiliti nell'Unione;
 - g) il numero di utenti finali registrati.
-

RECTIFICATIE

**van Verordening (EU) van het Europees Parlement en de Raad van 13 juni 2024 tot
vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging
van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013,
(EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU,
(EU) 2016/797 en (EU) 2020/1828
(verordening artificiële intelligentie)**

(PE-CONS 24/1/24 REV 1 van 14 juni 2024)

De tekst van PE-CONS 24/24 wordt vervangen door de volgende tekst:

“VERORDENING (EU) 2024/...
VAN HET EUROPEES PARLEMENT EN DE RAAD

van 13 juni 2024

**tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie
en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013,
(EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144
en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828
(verordening artificiële intelligentie)**

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name de artikelen 16 en 114,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité¹,

Gezien het advies van de Europese Centrale Bank²,

Gezien het advies van het Comité van de Regio's³,

Handelend volgens de gewone wetgevingsprocedure⁴,

¹ PB C 517 van 22.12.2021, blz. 56.

² PB C 115 van 11.3.2022, blz. 5.

³ PB C 97 van 28.2.2022, blz. 60.

⁴ Standpunt van het Europees Parlement van 13 maart 2024 (nog niet bekendgemaakt in het Publicatieblad) en besluit van de Raad van 21 mei 2024.

Overwegende hetgeen volgt:

- (1) Deze verordening heeft ten doel de werking van de interne markt te verbeteren door een uniform rechtskader vast te stellen, met name voor de ontwikkeling, het in de handel brengen, het in gebruik stellen, en het gebruik van artificiële-intelligentiesystemen (AI-systemen) in de Unie, in overeenstemming met de waarden van de Unie, de introductie van mensgerichte en betrouwbare artificiële intelligentie (AI) te bevorderen en te zorgen voor een hoge mate van bescherming van de gezondheid, de veiligheid en de grondrechten zoals vastgelegd in het Handvest van de grondrechten van de Europese Unie (het “Handvest”), met inbegrip van de democratie, de rechtsstaat en de bescherming van het milieu, te beschermen tegen de schadelijke effecten van AI-systemen in de Unie, alsook innovatie te ondersteunen. Deze verordening waarborgt het vrije verkeer van op AI gebaseerde goederen en diensten over de grenzen heen, zodat de lidstaten geen beperkingen kunnen opleggen aan de ontwikkeling, het in de handel brengen en het gebruik van AI-systemen, tenzij dat door deze verordening uitdrukkelijk wordt toegestaan.
- (2) Deze verordening moet worden toegepast in overeenstemming met de in het Handvest vastgelegde waarden van de Unie, om zo de bescherming van natuurlijke personen, ondernemingen, de democratie, de rechtsstaat en de bescherming van het milieu te faciliteren en tegelijkertijd innovatie en werkgelegenheid te stimuleren en van de Unie een voortrekker te maken bij de introductie van betrouwbare AI.

- (3) AI-systemen kunnen gemakkelijk worden ingezet in een ruime verscheidenheid van economische sectoren en in tal van onderdelen van de samenleving, ook grensoverschrijdend, en kunnen gemakkelijk in de hele Unie circuleren. Bepaalde lidstaten hebben reeds overwogen om nationale regels vast te stellen om ervoor te zorgen dat AI betrouwbaar en veilig is en wordt ontwikkeld en gebruikt met inachtneming van de verplichtingen inzake de grondrechten. Onderling afwijkende nationale regels kunnen leiden tot versnippering van de interne markt en tot vermindering van de rechtszekerheid voor operatoren die AI-systemen ontwikkelen, importeren of gebruiken. Daarom moet in de hele Unie een consistent en hoog beschermingsniveau worden gewaarborgd zodat AI betrouwbaar is, terwijl verschillen die het vrije verkeer, de innovatie, de inzet en de ingebruikneming van AI-systemen en aanverwante producten en diensten op de interne markt belemmeren, moeten worden voorkomen door uniforme verplichtingen voor operatoren vast te stellen en op de hele interne markt een eenvormige eerbiediging van dwingende redenen van algemeen belang en van de rechten van personen te waarborgen op basis van artikel 114 van het Verdrag betreffende de werking van de Europese Unie (VWEU). Voor zover deze verordening specifieke regels bevat inzake de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, waarbij beperkingen worden opgelegd aan het voor rechtshandhaving bedoelde gebruik van AI-systemen voor biometrische identificatie op afstand, AI-systemen voor risicobeoordelingen van natuurlijke personen en AI-systemen voor biometrische categorisering, moet deze verordening, wat die specifieke regels betreft, worden gebaseerd op artikel 16 VWEU. In het licht van deze specifieke regels en het gebruik van artikel 16 VWEU is het aangewezen het Europees Comité voor gegevensbescherming te raadplegen.

- (4) AI is een snel evoluerende verzameling van technologieën die bijdraagt aan een brede waaier van economische, milieu- en maatschappelijke voordelen in alle industrieën en sociale activiteiten. Het gebruik van AI kan ondernemingen, dankzij verbeterde voorspellingen, geoptimaliseerde verrichtingen en toewijzing van middelen en gepersonaliseerde digitale oplossingen voor natuurlijke personen en organisaties een belangrijk concurrentievoordeel opleveren en helpen om sociaal en ecologische gunstige resultaten te behalen, bijvoorbeeld in de gezondheidszorg, de landbouw, voedselveiligheid, onderwijs en opleiding, media, sport, cultuur, infrastructuurbeheer, energie, vervoer en logistiek, openbare diensten, veiligheid, justitie, efficiënt gebruik van hulpbronnen en energie, milieumonitoring, behoud en herstel van biodiversiteit en ecosystemen en klimaatmitigatie en -adaptatie.
- (5) Tegelijkertijd kan AI, afhankelijk van de omstandigheden waarin ze wordt toegepast en gebruikt, en van het niveau van technologische ontwikkeling, risico's opleveren en schade toebrengen aan de openbare belangen en grondrechten die door de Uniewetgeving worden beschermd. Deze schade kan materieel of immaterieel zijn, en kan lichamelijke, psychische, maatschappelijke of economische schade omvatten.

- (6) Aangezien AI van grote invloed op de samenleving kan zijn en het dus nodig is vertrouwen op te bouwen, is het essentieel dat AI en het AI-regelgevingskader worden ontwikkeld in overeenstemming met de waarden van de Unie zoals verankerd in artikel 2 van het Verdrag betreffende de Europese Unie (VEU), met de in de Verdragen vastgelegde grondrechten en fundamentele vrijheden, alsook, op grond van artikel 6 VEU, met het Handvest. Een eerste voorwaarde is dat AI een mensgerichte technologie moet zijn. Het moet dienen als instrument voor mensen, met als uiteindelijk doel het welzijn van de mens te vergroten.
- (7) Teneinde een consistent en hoog niveau van bescherming van de openbare belangen op het gebied van gezondheid, veiligheid en grondrechten te garanderen, moeten gemeenschappelijke regels voor AI-systemen met een hoog risico worden vastgesteld. Die regels moeten in overeenstemming zijn met het Handvest, niet-discriminerend zijn en stroken met de internationale handelsverbintenissen van de Unie. In de regels moet ook rekening worden gehouden met de Europese verklaring over digitale rechten en beginselen voor het digitale decennium en de ethische richtsnoeren voor betrouwbare KI van de deskundigengroep op hoog niveau inzake artificiële intelligentie (AI HLEG).

- (8) Om de ontwikkeling, het gebruik en de introductie van AI op de interne markt te bevorderen is daarom een rechtskader van de Unie nodig met geharmoniseerde regels inzake AI, dat tegelijkertijd de openbare belangen in hoge mate beschermt, bijvoorbeeld op het gebied van gezondheid en veiligheid en de bescherming van de grondrechten, met inbegrip van de democratie, de rechtsstaat en de bescherming van het milieu, zoals die worden erkend en beschermd door de Uniewetgeving. Om dat doel te bereiken, moeten regels worden vastgesteld voor het in de handel brengen, het in gebruik stellen en het gebruik van bepaalde AI-systemen, zodat de goede werking van de interne markt wordt gewaarborgd en deze systemen kunnen profiteren van het beginsel van vrij verkeer van goederen en diensten. Die regels moeten duidelijk en robuust zijn voor wat betreft de bescherming van de grondrechten, en nieuwe innovatieve oplossingen ondersteunen, om zo een Europees ecosysteem mogelijk te maken van publieke en particuliere actoren die AI-systemen creëren conform de waarden van de Unie, en het potentieel van de digitale transformatie in alle regio's van de Unie te ontsluiten. Door die regels, alsook maatregelen ter ondersteuning van innovatie met bijzondere nadruk op kleine en middelgrote ondernemingen (kmo's), waaronder start-ups, vast te stellen, steunt deze verordening de doelstelling om de Europese mensgerichte benadering van AI te bevorderen en wereldwijd een voortrekkersrol te spelen bij de ontwikkeling van veilige, betrouwbare en ethische AI, zoals verklaard door de Europese Raad⁵, en waarborgt deze verordening de bescherming van ethische beginselen, zoals specifiek gevraagd door het Europees Parlement⁶.

⁵ Europese Raad, Buitengewone bijeenkomst van de Europese Raad (1 en 2 oktober 2020) – Conclusies, EUCO 13/20, 2020, blz. 6.

⁶ Resolutie van het Europees Parlement van 20 oktober 2020 met aanbevelingen aan de Commissie betreffende een kader voor ethische aspecten van artificiële intelligentie, robotica en aanverwante technologieën, 2020/2012(INL).

- (9) Er moeten geharmoniseerde regels worden vastgesteld die van toepassing zijn op het in de handel brengen, in gebruik stellen en gebruiken van AI-systemen met een hoog risico, en in overeenstemming zijn met Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad⁷, Besluit nr. 768/2008/EG van het Europees Parlement en de Raad⁸ en Verordening (EU) 2019/1020 van het Europees Parlement en de Raad⁹ (“het nieuwe wetgevingskader”). De in deze verordening vastgelegde geharmoniseerde regels moeten in alle sectoren van toepassing zijn en mogen, in overeenstemming met het nieuwe wetgevingskader, geen afbreuk doen aan bestaand Unierecht, met name het Unierecht inzake gegevensbescherming, consumentenbescherming, grondrechten, werkgelegenheid, bescherming van werknemers en productveiligheid, waarop deze verordening een aanvulling vormt. Bijgevolg blijven alle rechten en rechtsmiddelen waarin dat Unierecht voorziet voor consumenten en andere personen voor wie AI-systemen negatieve gevolgen kunnen hebben, onder meer wat betreft de vergoeding van mogelijke schade overeenkomstig Richtlijn 85/374/EEG van de Raad¹⁰, onverlet en volledig van toepassing.

⁷ Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en tot intrekking van Verordening (EEG) nr. 339/93 (PB L 218 van 13.8.2008, blz. 30).

⁸ Besluit nr. 768/2008/EG van het Europees Parlement en de Raad van 9 juli 2008 betreffende een gemeenschappelijk kader voor het verhandelen van producten en tot intrekking van Besluit 93/465/EEG van de Raad (PB L 218 van 13.8.2008, blz. 82).

⁹ Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 (PB L 169 van 25.6.2019, blz. 1).

¹⁰ Richtlijn 85/374/EEG van de Raad van 25 juli 1985 betreffende de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen der lidstaten inzake de aansprakelijkheid voor producten met gebreken (PB L 210 van 7.8.1985, blz. 29).

Voorts mag deze verordening, in het kader van de werkgelegenheid en de bescherming van werknemers, derhalve geen afbreuk doen aan het recht van de Unie inzake sociaal beleid, noch aan het nationale arbeidsrecht, in naleving van het Unierecht, wat betreft werkgelegenheid en arbeidsvoorwaarden, met inbegrip van gezondheid en veiligheid op het werk en de betrekkingen tussen werkgevers en werknemers. Deze verordening mag evenmin afbreuk doen aan de uitoefening van de in de lidstaten en op het niveau van de Unie erkende grondrechten, waaronder het stakingsrecht of de stakingsvrijheid dan wel het recht of de vrijheid om in het kader van de specifieke stelsels van arbeidsverhoudingen in de lidstaten andere acties te voeren, alsook het recht om over collectieve overeenkomsten te onderhandelen, deze te sluiten en naleving ervan af te dwingen, of om collectieve actie te voeren overeenkomstig het nationaal recht. Deze verordening mag geen afbreuk doen aan de bepalingen ter verbetering van de arbeidsomstandigheden bij platformwerk die zijn vastgelegd in een richtlijn van het Europees Parlement en de Raad betreffende de verbetering van de arbeidsvoorwaarden bij platformwerk. Daarnaast heeft deze verordening tot doel de doeltreffendheid van dergelijke bestaande rechten en rechtsmiddelen te versterken door specifieke eisen en verplichtingen vast te stellen, onder meer met betrekking tot de transparantie, technische documentatie en registratie van AI-systemen. Voorts moeten de verplichtingen die verschillende operatoren die betrokken zijn bij de AI-waardeketen uit hoofde van deze verordening krijgen opgelegd, van toepassing zijn onverminderd het nationale recht, in naleving van het Unierecht, met als gevolg dat het gebruik van bepaalde AI-systemen wordt beperkt indien dergelijk nationaal recht buiten het toepassingsgebied van deze verordening valt of andere legitieme doelstellingen van algemeen belang nastreeft dan die welke door deze verordening worden nagestreefd. Deze verordening mag bijvoorbeeld geen afbreuk doen aan het nationale arbeidsrecht en de wetgeving inzake de bescherming van minderjarigen, namelijk personen jonger dan 18 jaar, rekening houdend met algemene opmerking nr. 25 (2021) bij het Verdrag van de Verenigde Naties inzake de rechten van het kind over kinderrechten met betrekking tot de digitale omgeving, voor zover deze niet specifiek zijn voor AI-systemen en andere legitieme doelstellingen van algemeen belang nastreven.

- (10) Het grondrecht van de bescherming van persoonsgegevens wordt met name gewaarborgd door de Verordeningen (EU) 2016/679¹¹ en (EU) 2018/1725¹² van het Europees Parlement en de Raad en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad¹³. Daarnaast beschermt Richtlijn 2002/58/EG van het Europees Parlement en de Raad¹⁴ het privéleven en de vertrouwelijkheid van communicatie, onder meer door te voorzien in voorwaarden met betrekking tot de opslag van en de toegang tot persoonsgegevens en niet-persoonsgebonden gegevens in eindapparatuur. Die rechtshandelingen van de Unie vormen de basis voor duurzame en verantwoorde dataverwerking, onder meer wanneer datasets een mix van persoonsgegevens en niet-persoonsgebonden gegevens bevatten. Deze verordening laat de toepassing van de bestaande Uniewetgeving betreffende de verwerking van persoonsgegevens, met inbegrip van de taken en bevoegdheden van de onafhankelijke toezichthoudende autoriteiten die met het toezicht op de naleving van die instrumenten belast zijn, onverlet.

¹¹ Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

¹² Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

¹³ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

¹⁴ Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

Deze verordening doet evenmin afbreuk aan de verplichtingen van aanbieders en gebruiksverantwoordelijken van AI-systemen in hun rol als verwerkingsverantwoordelijke of verwerker die voortvloeien uit het Unie- of nationale recht inzake de bescherming van persoonsgegevens, voor zover er in het kader van het ontwerp, de ontwikkeling of het gebruik van AI-systemen persoonsgegevens worden verwerkt. Het is ook passend te verduidelijken dat betrokkenen alle rechten en waarborgen blijven genieten die hun door dat Unierecht zijn toegekend, met inbegrip van de rechten die verband houden met uitsluitend geautomatiseerde individuele besluitvorming, waaronder profilering. De in deze verordening vastgelegde geharmoniseerde regels voor het in de handel brengen, de ingebruikstelling en het gebruik van AI-systemen moeten de doeltreffende uitvoering vergemakkelijken en de uitoefening van de rechten en andere rechtsmiddelen van betrokkenen mogelijk maken die worden gewaarborgd door het Unierecht inzake de bescherming van persoonsgegevens en andere grondrechten.

- (11) Deze verordening mag geen afbreuk doen aan de bepalingen betreffende de aansprakelijkheid van aanbieders van tussenhandelsdiensten, zoals vastgelegd in Verordening 2022/2065 van het Europees Parlement en de Raad¹⁵.

¹⁵ Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van Richtlijn 2000/31/EG (digitaledienstenverordening) (PB L 277 van 27.10.2022, blz. 1).

- (12) Het begrip “AI-systeem” in deze verordening moet duidelijk worden gedefinieerd en moet nauw aansluiten op het werk van internationale organisaties die zich bezighouden met AI, om rechtszekerheid te waarborgen, internationale convergentie en brede acceptatie te faciliteren, en tegelijkertijd de nodige flexibiliteit te bieden om op de snelle technologische ontwikkelingen op dit gebied te kunnen inspelen. Bovendien moet de definitie gebaseerd zijn op de belangrijkste kenmerken van AI-systemen die het onderscheiden van eenvoudigere traditionele softwaresystemen of programmeringsbenaderingen, en mag het geen betrekking hebben op systemen die gebaseerd zijn op regels die uitsluitend door natuurlijke personen zijn vastgesteld om automatisch handelingen uit te voeren. Een belangrijk kenmerk van AI-systemen is hun inferentievermogen. Dit inferentievermogen slaat op het proces waarbij output, zoals voorspellingen, content, aanbevelingen of besluiten, wordt verkregen waarmee fysieke en virtuele omgevingen kunnen worden beïnvloed, en op het vermogen van AI-systemen om modellen of algoritmen, of beide, af te leiden uit input of data. De technieken die inferentie mogelijk maken bij de opbouw van een AI-systeem, omvatten benaderingen op basis van machinaal leren waarbij aan de hand van data wordt geleerd hoe bepaalde doelstellingen kunnen worden bereikt, alsook op logica en kennis gebaseerde benaderingen waarbij iets wordt geïnfereerd uit gecodeerde kennis of uit een symbolische weergave van de op te lossen taak. Het inferentievermogen van een AI-systeem overstijgt de elementaire verwerking van data door leren, redeneren of modelleren mogelijk te maken. De term “op een machine gebaseerd” verwijst naar het feit dat AI-systemen op machines draaien.

De verwijzing naar expliciete of impliciete doelstellingen onderstreept dat AI-systemen kunnen functioneren volgens expliciete, gedefinieerde doelstellingen, of volgens impliciete doelstellingen. De doelstellingen van een AI-systeem kunnen verschillen van het beoogde doel van het AI-systeem in een specifieke context. Voor de toepassing van deze verordening moeten onder omgevingen de contexten worden verstaan waarin de AI-systemen werken, terwijl de output die door het AI-systeem wordt gegenereerd een uiting is van de verschillende functies van AI-systemen en de vorm kan aannemen van voorspellingen, content, aanbevelingen of besluiten. AI-systemen worden zodanig ontworpen dat zij in verschillende mate autonoom kunnen functioneren, wat betekent dat zij een zekere mate van onafhankelijkheid van menselijke betrokkenheid bezitten en zonder menselijke tussenkomst kunnen functioneren. Het aanpassingsvermogen dat een AI-systeem na het inzetten ervan kan vertonen, heeft betrekking op zelflerende capaciteiten, waardoor het systeem tijdens het gebruik kan veranderen. AI-systemen kunnen op standalonebasis of als component van een product worden gebruikt, ongeacht of het systeem fysiek in het product is geïntegreerd (ingebed) dan wel ten dienste staat van de functionaliteit van het product zonder daarin te zijn geïntegreerd (niet-ingebed).

- (13) Het in deze verordening bedoelde begrip “gebruiksverantwoordelijke” moet worden uitgelegd als alle natuurlijke of rechtspersonen, met inbegrip van overheidsinstanties, agentschappen of andere organen, die een AI-systeem onder eigen verantwoordelijkheid gebruiken, behalve in gevallen waarin het AI-systeem wordt gebruikt in het kader van een persoonlijke niet-professionele activiteit. Afhankelijk van het type AI-systeem kan het gebruik van het systeem invloed hebben op andere personen dan de gebruiksverantwoordelijke.
- (14) Het in deze verordening gebruikte begrip “biometrische gegevens” moet worden uitgelegd in het licht van het begrip biometrische gegevens zoals gedefinieerd in artikel 4, punt 14), van Verordening (EU) 2016/679, artikel 3, punt 18), van Verordening (EU) 2018/1725 en artikel 3, punt 13), van Richtlijn (EU) 2016/680. Biometrische gegevens kunnen de authenticatie, identificatie of categorisering van natuurlijke personen en de herkenning van emoties van natuurlijke personen mogelijk maken.
- (15) Het in deze verordening bedoelde begrip “biometrische identificatie” moet worden gedefinieerd als de automatische herkenning van fysieke, fysiologische en gedragsgerelateerde menselijke kenmerken zoals het gezicht, oogbewegingen, lichaamsvorm, stem, prosodie, gang, houding, hartslag, bloeddruk, geur, toetsaanslagen, met als doel de identiteit van een natuurlijke persoon vast te stellen door biometrische gegevens van die natuurlijke persoon te vergelijken met opgeslagen biometrische gegevens van natuurlijke personen in een referentiedatabank, ongeacht of die natuurlijke persoon daarmee heeft ingestemd. Daarvan uitgesloten zijn AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie, met inbegrip van authenticatie, die er uitsluitend op gericht zijn te bevestigen dat een specifieke natuurlijke persoon daadwerkelijk de persoon is die hij of zij beweert te zijn, en de identiteit van een natuurlijke persoon te bevestigen met als enige doel toegang te verschaffen tot een dienst, een apparaat te ontgrendelen of beveiligde toegang te verschaffen tot een locatie.

- (16) Het begrip “biometrische categorisering” in deze verordening moet worden gedefinieerd als het toewijzen van natuurlijke personen aan specifieke categorieën op basis van hun biometrische gegevens. Zulke specifieke categorieën kunnen betrekking hebben op aspecten zoals geslacht, leeftijd, haarkleur, oogkleur, tatoeages, gedragsgerelateerde of persoonlijkheidskenmerken, taal, religie, het behoren tot een nationale minderheid, seksuele gerichtheid of politieke overtuiging. Daarvan uitgesloten zijn systemen voor biometrische categorisering die een louter bijkomstige functie zijn die intrinsiek verbonden is met een andere commerciële dienst, waarbij die functie om objectieve technische redenen niet los van de hoofddienst kan worden gebruikt, en de integratie van die functie of functionaliteit geen middel is om de toepassing van de regels van deze verordening te omzeilen. Filters die op onlinemarktplaatsen gebruikte gezichts- of lichaamskenmerken categoriseren, kunnen bijvoorbeeld een dergelijke nevenfunctie vormen, aangezien zij alleen kunnen worden gebruikt voor de hoofddienst die bestaat in de verkoop van een product door de consument in staat te stellen de weergave van het product op zichzelf te bekijken en de consument te helpen een aankoopbeslissing te nemen. Filters die worden gebruikt op online socialenetwerkdiensten die gezichts- of lichaamskenmerken categoriseren om gebruikers in staat te stellen foto's of video's toe te voegen of te wijzigen, kunnen ook als bijkomstig worden beschouwd, aangezien dergelijke filters niet kunnen worden gebruikt zonder de hoofddienst van de socialenetwerkdiensten die bestaat in het online delen van content.

- (17) Het in deze verordening bedoelde begrip “systeem voor biometrische identificatie op afstand” moet functioneel worden gedefinieerd, als een AI-systeem dat bedoeld is voor de identificatie van natuurlijke personen, doorgaans van een afstand, zonder dat zij hier actief bij betrokken zijn, door vergelijking van de biometrische gegevens van een persoon met de biometrische gegevens die zijn opgenomen in een referentiedatabank, ongeacht de specifieke gebruikte technologie, processen of soorten biometrische gegevens. Dergelijke systemen voor biometrische identificatie op afstand worden doorgaans gebruikt om meerdere personen of hun gedrag gelijktijdig waar te nemen, teneinde de identificatie van natuurlijke personen, zonder dat zij er actief bij betrokken zijn, aanzienlijk te vergemakkelijken. Daarvan uitgesloten zijn AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie, met inbegrip van authenticatie, met als enige doel te bevestigen dat een specifieke natuurlijke persoon daadwerkelijk de persoon is die hij of zij beweert te zijn, en de identiteit van een natuurlijke persoon te bevestigen met als enige doel toegang te verschaffen tot een dienst, een apparaat te ontgrendelen of beveiligde toegang te verschaffen tot een locatie. Die uitsluiting wordt gerechtvaardigd door het feit dat dergelijke systemen waarschijnlijk geringe gevolgen zullen hebben voor de grondrechten van natuurlijke personen in vergelijking met systemen voor biometrische identificatie op afstand die kunnen worden gebruikt voor de verwerking van biometrische gegevens van een groot aantal personen, zonder dat zij er actief bij betrokken zijn. In het geval van realsystemen gebeurt de vastlegging van de biometrische gegevens, de vergelijking en de identificatie allemaal ogenblikkelijk, bijna ogenblikkelijk of in ieder geval zonder noemenswaardige vertraging. In dit verband mag er geen ruimte zijn om de regels van deze verordening betreffende het realtimegebruik van de betrokken AI-systemen te omzeilen door kleine vertragingen toe te staan. Bij realsystemen wordt gebruik gemaakt van: “live” of “bijna live” materiaal, zoals videobeelden, die worden gegenereerd door een camera of een ander toestel met soortgelijke functionaliteit. In het geval van systemen “achteraf” zijn de biometrische gegevens daarentegen reeds vastgelegd en vinden de vergelijking en de identificatie pas met een noemenswaardige vertraging plaats. Het gaat dan om materiaal, zoals foto's of videobeelden gegenereerd door camera's van een gesloten televisiecircuit of privétoestellen, dat vóór het gebruik van het systeem is gegenereerd met betrekking tot de betrokken natuurlijke personen.

- (18) Het in deze verordening bedoelde begrip “systeem voor het herkennen van emoties” moet worden gedefinieerd als een AI-systeem dat is bedoeld voor het vaststellen of afleiden van de emoties of intenties van natuurlijke personen op basis van hun biometrische gegevens. Het begrip verwijst naar emoties of intenties zoals geluk, droefheid, woede, verrassing, weersin, verlegenheid, opwinding, schaamte, minachting, tevredenheid en plezier. Het omvat geen fysieke toestanden, zoals pijn of vermoeidheid, met inbegrip van bijvoorbeeld systemen die worden gebruikt om vermoeidheid bij beroepspiloten of beroepschauffeurs te detecteren om ongevallen te voorkomen. Het omvat evenmin de loutere detectie van gemakkelijk zichtbare uitdrukkingen, gebaren of bewegingen, tenzij deze worden gebruikt om emoties te herkennen of af te leiden. Die uitdrukkingen kunnen basale gezichtsuitdrukkingen zijn, zoals een frons of een glimlach, of gebaren zoals hand-, arm-, of hoofdbewegingen, of kenmerken van iemands stem, zoals een luide spreektoon of een fluisterton.

- (19) Voor de toepassing van deze verordening moet het begrip “openbare ruimte” worden opgevat als een verwijzing naar elke fysieke plaats die toegankelijk is voor een onbepaald aantal natuurlijke personen, ongeacht of de plaats in kwestie particulier of publiek eigendom is, ongeacht de activiteit waarvoor de plaats kan worden gebruikt, zoals voor handel, zoals winkels, restaurants, cafés, voor diensten, zoals banken, beroepsactiviteiten, horeca, voor sport, zoals zwembaden, fitnesscentra, stadions, voor vervoer, zoals bus-, metro- en treinstations, luchthavens, vervoermiddelen, voor ontspanning, zoals bioscopen, theaters, musea, concert- en conferentiezalen of voor vrijetijdsbesteding of anderszins, zoals openbare wegen en pleinen, parken, bossen, speelplaatsen. Een plaats moet ook als openbare ruimte worden ingedeeld indien, ongeacht potentiële capaciteits- of beveiligingsbeperkingen, de toegang onderworpen is aan bepaalde vooraf vastgestelde voorwaarden waaraan een onbepaald aantal personen kan voldoen, zoals de aankoop van een vervoerbewijs of een vervoerstitel, voorafgaande registratie of het hebben van een bepaalde leeftijd. Een plaats mag daarentegen niet als openbare ruimte worden beschouwd indien de toegang beperkt is tot specifieke en gedefinieerde natuurlijke personen door middel van Unie- of nationale wetgeving die rechtstreeks verband houdt met de openbare veiligheid of beveiliging of door de duidelijke wilsuiting van de persoon die ter plaatse over de benodigde autoriteit beschikt. De feitelijke mogelijkheid van toegang alleen, zoals een onvergrendelde deur of een open poort in een omheining, betekent niet dat de plaats een openbare ruimte is wanneer er aanwijzingen of omstandigheden zijn die het tegendeel suggereren, zoals borden die de toegang verbieden of beperken. Bedrijfsruimten en fabrieksgebouwen, alsook kantoren en werkplekken die alleen bestemd zijn voor bevoegde werknemers en dienstverleners, zijn plaatsen die niet openbaar zijn. Gevangenissen of grenstoezichtsgebieden mogen niet als openbare ruimte worden ingedeeld. Sommige andere plaatsen kunnen uit zowel niet-openbare als openbare ruimten bestaan, zoals de hal van een particulier woongebouw waar men door moet om bij een arts te komen, of een luchthaven. Onlineruimten vallen onder het toepassingsgebied, omdat het geen fysieke ruimten zijn. Of een bepaalde ruimte openbaar is, moet echter per geval worden bepaald, rekening houdend met de specifieke omstandigheden van de situatie in kwestie.

- (20) Om de grootste voordelen van AI-systemen te behalen en tegelijkertijd de grondrechten, gezondheid en veiligheid te beschermen en democratische controle mogelijk te maken, moeten aanbieders, gebruiksverantwoordelijken en betrokken personen door middel van AI-geletterdheid van de nodige kennis voorzien worden om onderbouwde beslissingen te nemen met betrekking tot AI-systemen. Die kennis kan verschillen naargelang de context en kan inzicht omvatten in de correcte toepassing van technische elementen tijdens de ontwikkelingsfase van het AI-systeem, de maatregelen die moeten worden toegepast tijdens het gebruik ervan, hoe de output van het AI-systeem moet worden geïnterpreteerd, en, in het geval van betrokken personen, de kennis die nodig is om te begrijpen hoe beslissingen die met behulp van AI worden genomen, op hen van invloed zullen zijn. In het kader van de toepassing van deze verordening moet AI-geletterdheid alle relevante actoren in de AI-waardeketen de inzichten verschaffen die nodig zijn om de passende naleving en de correcte handhaving ervan te waarborgen. Voorts kunnen de brede uitvoering van maatregelen op het gebied van AI-geletterdheid en de invoering van passende vervolgmaatregelen bijdragen tot het verbeteren van de arbeidsomstandigheden en uiteindelijk de consolidatie en innovatie van betrouwbare AI in de Unie ondersteunen. De Europese raad voor artificiële intelligentie (European Artificial Intelligence Board -de “AI-board”) moet de Commissie ondersteunen bij het bevorderen van instrumenten voor AI-geletterdheid en van de bekendheid van het publiek met en hun begrip van de voordelen, risico's, waarborgen, rechten en plichten met betrekking tot het gebruik van AI-systemen. In samenwerking met de relevante belanghebbenden moeten de Commissie en de lidstaten de opstelling van vrijwillige gedragscodes faciliteren om de AI-geletterdheid te bevorderen bij personen die zich bezighouden met de ontwikkeling, de exploitatie en het gebruik van AI.

- (21) Om een gelijk speelveld en een doeltreffende bescherming van de rechten en vrijheden van natuurlijke personen in heel de Unie te garanderen, moeten de bij deze verordening vastgestelde regels zonder discriminatie van toepassing zijn op aanbieders van AI-systemen, ongeacht of zij in de Unie of in een derde land gevestigd zijn, en op in de Unie gevestigde gebruiksverantwoordelijken van AI-systemen.
- (22) Gezien hun digitale aard moeten zelfs bepaalde AI-systemen die niet in de Unie in de handel worden gebracht, in gebruik worden gesteld of worden gebruikt, onder het toepassingsgebied van deze verordening vallen. Dit is bijvoorbeeld het geval wanneer een in de Unie gevestigde operator aan een in een derde land gevestigde operator bepaalde diensten uitbestedt voor een activiteit die wordt verricht door een AI-systeem dat als een AI-systeem met een hoog risico kan worden aangemerkt. In die omstandigheden zou het AI-systeem dat door de operator in een derde land wordt gebruikt, data kunnen verwerken die rechtmatig in de Unie zijn verzameld en vanuit de Unie zijn doorgegeven, en vervolgens de aanbestedende operator in de Unie kunnen voorzien van de output van dat AI-systeem die het resultaat is van die verwerking, zonder dat het AI-systeem in de Unie in de handel wordt gebracht, in gebruik wordt gesteld of wordt gebruikt. Om te voorkomen dat deze verordening wordt omzeild en om natuurlijke personen die zich in de Unie bevinden doeltreffend te beschermen, moet deze verordening ook van toepassing zijn op aanbieders en gebruiksverantwoordelijken van AI-systemen die in een derde land zijn gevestigd, voor zover de door die systemen geproduceerde output bedoeld is om in de Unie te worden gebruikt.

Om rekening te houden met bestaande regelingen en bijzondere behoeften inzake toekomstige samenwerking met buitenlandse partners waarmee informatie en bewijsmateriaal worden uitgewisseld, mag deze verordening evenwel niet van toepassing zijn op overheidsinstanties van een derde land en internationale organisaties wanneer zij optreden in het kader van samenwerking of internationale overeenkomsten die op het niveau van de Unie of op nationaal niveau zijn gesloten met het oog op samenwerking met de Unie of haar lidstaten op het gebied van rechtshandhaving en justitie, mits het betrokken derde land of de betrokken internationale organisatie in passende waarborgen voorziet met betrekking tot de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke personen. In voorkomend geval kan dit betrekking hebben op activiteiten van entiteiten die door derde landen zijn belast met de uitvoering van specifieke taken ter ondersteuning van deze samenwerking op het gebied van rechtshandhaving en justitie. Een dergelijk kader voor samenwerking of dergelijke overeenkomsten zijn bilateraal gesloten tussen lidstaten en derde landen of tussen de Europese Unie, Europol en andere agentschappen van de Unie enerzijds en derde landen en internationale organisaties anderzijds. De autoriteiten die uit hoofde van deze verordening bevoegd zijn voor het toezicht op de rechtshandhavinginstanties en justitiële autoriteiten, moeten beoordelen of die kaders voor samenwerking of internationale overeenkomsten passende waarborgen bevatten met betrekking tot de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke personen. De ontvangende nationale autoriteiten en de ontvangende instellingen, organen en instanties van de Unie die gebruikmaken van dergelijke output in de Unie, blijven er verantwoordelijk voor dat het gebruik ervan in overeenstemming is met het recht van de Unie. Wanneer die internationale overeenkomsten worden herzien of er in de toekomst nieuwe worden gesloten, moeten de overeenkomstsluitende partijen alles in het werk stellen om die overeenkomsten in overeenstemming te brengen met de eisen van deze verordening.

- (23) Deze verordening moet ook van toepassing zijn op instellingen, organen en instanties van de Unie wanneer zij optreden als aanbieder of gebruiksverantwoordelijke van een AI-systeem.

- (24) Indien en voor zover AI-systemen voor militaire, defensie- of nationale veiligheidsdoeleinden, met of zonder wijziging van die systemen, in de handel worden gebracht, in gebruik worden gesteld of worden gebruikt, moeten deze worden uitgesloten van het toepassingsgebied van deze verordening, ongeacht welk soort entiteit, bv. een publieke of private entiteit, die activiteiten uitvoert. Wat militaire en defensiedoeleinden betreft, wordt een dergelijke uitsluiting zowel gerechtvaardigd door artikel 4, lid 2, VEU, als door de specifieke kenmerken van het defensiebeleid van de lidstaten en het gemeenschappelijk defensiebeleid van de Unie krachtens titel V, hoofdstuk 2, VEU, die onder het internationaal publiekrecht vallen, wat derhalve het geschiktere rechtskader is voor de regulering van AI-systemen in de context van het gebruik van dodelijk geweld en andere AI-systemen in de context van militaire en defensieactiviteiten. Wat de doeleinden van nationale veiligheid betreft, wordt de uitsluiting zowel gerechtvaardigd door het feit dat nationale veiligheid overeenkomstig artikel 4, lid 2, VEU, de uitsluitende verantwoordelijkheid van elke lidstaat blijft, als door de specifieke aard en operationele behoeften van de nationale veiligheidsactiviteiten en door de specifieke nationale regels die op die activiteiten van toepassing zijn. Indien echter een AI-systeem dat is ontwikkeld, in de handel is gebracht, in gebruik is gesteld of wordt gebruikt voor militaire, defensie- of nationale veiligheidsdoeleinden, tijdelijk of permanent voor andere dan die doeleinden wordt gebruikt, bijvoorbeeld civiele of humanitaire doeleinden, rechtshandhaving of openbare veiligheid, valt een dergelijk systeem wel binnen het toepassingsgebied van deze verordening. In dat geval moet de entiteit die het AI-systeem voor andere doeleinden dan militaire, defensie- of nationale veiligheidsdoeleinden gebruikt, ervoor zorgen dat het AI-systeem voldoet aan deze verordening, tenzij dat reeds het geval is. AI-systemen die in de handel worden gebracht of in gebruik worden gesteld voor een uitgesloten doeleinde, d.w.z. militaire, defensie- of nationale veiligheidsdoeleinden, en een of meer niet-uitgesloten doeleinden, zoals civiele doeleinden of rechtshandhaving, vallen binnen het toepassingsgebied van deze verordening, en aanbieders van die systemen moeten er dan ook voor zorgen dat deze verordening wordt nageleefd. In die gevallen mag het feit dat een AI-systeem onder het toepassingsgebied van deze verordening valt, geen afbreuk doen aan de mogelijkheid voor entiteiten die nationale veiligheids-, defensie- en militaire activiteiten verrichten, ongeacht het soort entiteit dat die activiteiten uitvoert, om de AI-systemen te gebruiken voor nationale veiligheids-, militaire en defensiedoeleinden, waarvan het gebruik is uitgesloten van het toepassingsgebied van deze verordening. Een AI-systeem dat in de handel wordt gebracht voor civiele of rechtshandavingsdoeleinden en dat met of zonder wijziging wordt gebruikt voor militaire, defensie- of nationale veiligheidsdoeleinden, mag niet binnen het toepassingsgebied van deze verordening vallen, ongeacht het soort entiteit dat die activiteiten uitvoert.

- (25) Deze verordening moet innovatie ondersteunen en de vrijheid van wetenschap eerbiedigen en mag onderzoeks- en ontwikkelingsactiviteiten niet ondermijnen. Het is daarom noodzakelijk AI-systemen en -modellen die specifiek zijn ontwikkeld en in gebruik gesteld met wetenschappelijk onderzoek en wetenschappelijke ontwikkeling als enig doel, van het toepassingsgebied van deze verordening uit te sluiten. Bovendien moet ervoor worden gezorgd dat deze verordening geen andere gevolgen heeft voor wetenschappelijke onderzoeks- en ontwikkelingsactiviteiten met betrekking tot AI-systemen of -modellen voordat zij in de handel worden gebracht of in gebruik worden gesteld. Wat productgericht onderzoek en test- en ontwikkelingsactiviteiten met betrekking tot AI-systemen of -modellen betreft, mogen de bepalingen van deze verordening ook niet van toepassing zijn voordat die systemen en modellen in gebruik worden gesteld of in de handel worden gebracht. Die uitsluiting doet geen afbreuk aan de verplichting om aan deze verordening te voldoen wanneer een AI-systeem dat onder het toepassingsgebied van deze verordening valt, in de handel wordt gebracht of in gebruik wordt gesteld als gevolg van dergelijke onderzoeks- en ontwikkelingsactiviteiten, noch aan de toepassing van bepalingen inzake AI-testomgevingen voor regelgeving en testen onder reële omstandigheden. Onverminderd de uitsluiting van AI-systemen die specifiek zijn ontwikkeld en in gebruik gesteld met wetenschappelijk onderzoek en ontwikkeling als enig doel, moet elk ander AI-systeem dat voor de uitvoering van onderzoeks- en ontwikkelingsactiviteiten kan worden gebruikt, onderworpen blijven aan de bepalingen van deze verordening. Alle onderzoeks- en ontwikkelingsactiviteiten moeten in elk geval worden uitgevoerd met inachtneming van de erkende ethische en beroepsnormen voor wetenschappelijk onderzoek, en in overeenstemming met het toepasselijke Unierecht.

- (26) Om een evenredige en doeltreffende reeks bindende regels voor AI-systemen in te voeren, moet een duidelijk omschreven, risicogebaseerde aanpak worden gevolgd. Met die aanpak moet de aard en content van dergelijke regels worden afgestemd op de intensiteit en de omvang van de risico's die AI-systemen met zich mee kunnen brengen. Daarom is het noodzakelijk om bepaalde onaanvaardbare praktijken op het gebied van AI te verbieden, eisen voor AI-systemen met een hoog risico en verplichtingen voor de betrokken operatoren vast te stellen, en transparantieplichtingen voor bepaalde AI-systemen in te voeren.
- (27) Hoewel de risicogebaseerde aanpak de basis vormt voor een evenredige en doeltreffende reeks bindende regels, is het belangrijk te herinneren aan de ethische richtsnoeren voor betrouwbare KI van 2019 die zijn opgesteld door de onafhankelijke AI HLEG die door de Commissie is aangesteld. In die richtsnoeren heeft de AI HLEG zeven niet-bindende ethische beginselen ontwikkeld die ervoor moeten zorgen dat AI betrouwbaar en ethisch verantwoord is. Die beginselen zijn: invloed en toezicht door mensen, technische robuustheid en veiligheid, privacy en datagovernance, transparantie; diversiteit, non-discriminatie en rechtvaardigheid, sociaal en ecologisch welzijn, en verantwoordingsplicht. Onverminderd de juridisch bindende eisen van deze verordening en enig ander toepasselijk Unierecht dragen die richtsnoeren bij tot het ontwerpen van coherente, betrouwbare en mensgerichte AI, in overeenstemming met het Handvest en de waarden waarop de Unie is gegrondvest. Volgens de richtsnoeren van de AI HLEG houdt “invloed en toezicht door mensen” in dat AI-systemen worden ontwikkeld en gebruikt als een instrument dat ten dienste staat van mensen, dat de menselijke waardigheid en persoonlijke autonomie eerbiedigt, en dat functioneert op een wijze waar mensen op passende wijze controle en toezicht op kunnen houden.

“Technische robuustheid en veiligheid” betekent dat AI-systemen worden ontwikkeld op een wijze die voorziet in robuustheid in geval van problemen en in weerbaarheid tegen pogingen om het gebruik of de prestaties van het AI-systeem te wijzigen voor onrechtmatig gebruik door derden, en die onbedoelde schade tot een minimum beperkt.

“Privacy en datagovernance” betekent dat AI-systemen worden ontwikkeld en gebruikt in overeenstemming met de regels inzake privacy en gegevensbescherming, en de verwerking van gegevens voldoet aan hoge normen wat kwaliteit en integriteit betreft. “Transparantie” betekent dat AI-systemen worden ontwikkeld en gebruikt op een wijze die passende traceerbaarheid en verklaarbaarheid mogelijk maakt, waarbij mensen ervan bewust worden gemaakt dat zij communiceren of interageren met een AI-systeem, en gebruiksverantwoordelijken naar behoren worden geïnformeerd over de mogelijkheden en beperkingen van dat AI-systeem en betrokken personen worden geïnformeerd over hun rechten. “Diversiteit, non-discriminatie en rechtvaardigheid” betekent dat AI-systemen zodanig worden ontwikkeld en gebruikt dat de inclusie van diverse actoren wordt gewaarborgd en dat gelijke toegang, gendergelijkheid en culturele diversiteit worden bevorderd, waarbij discriminerende effecten en onrechtvaardige vertekeningen die op grond van het Unierecht of het nationale recht verboden zijn, worden voorkomen. “Sociaal en ecologisch welzijn” betekent dat AI-systemen worden ontwikkeld en gebruikt op een duurzame en milieuvriendelijke wijze en op een manier die alle mensen ten goede komt, waarbij de langetermijneffecten op het individu, de samenleving en de democratie worden gemonitord en beoordeeld. De toepassing van die beginselen moet waar mogelijk worden vertaald in het ontwerp en het gebruik van AI-modellen. Zij moeten in ieder geval dienen als basis voor het opstellen van gedragscodes in het kader van deze verordening. Alle belanghebbenden, met inbegrip van het bedrijfsleven, de academische wereld, het maatschappelijk middenveld en normalisatieorganisaties, worden aangemoedigd om in voorkomend geval rekening te houden met de ethische beginselen voor de ontwikkeling van vrijwillige beste praktijken en normen.

- (28) Afgezien van de vele nuttige toepassingen van AI kan zij ook worden misbruikt en nieuwe en krachtige instrumenten voor manipulatie, uitbuiting en sociale controle opleveren. Dergelijke praktijken zijn bijzonder schadelijk en abusief en moeten worden verboden omdat zij in strijd zijn met de waarden van de Unie, namelijk eerbied voor de menselijke waardigheid, vrijheid, gelijkheid, democratie en de rechtsstaat, en met de grondrechten van de Unie die zijn vastgelegd in het Handvest, waaronder het recht op non-discriminatie, gegevensbescherming en privacy, en de rechten van het kind.

- (29) Op AI gebaseerde manipulatietechnieken kunnen worden gebruikt om gebruikers te overtuigen zich ongewenst te gedragen en ze te misleiden door hen aan te zetten tot bepaalde beslissingen waardoor hun autonomie, besluitvorming en keuze worden ondermijnd en beperkt. Het in de handel brengen, in gebruik stellen of gebruiken van bepaalde AI-systemen met als doel of gevolg het menselijk gedrag wezenlijk te verstoren, waarbij waarschijnlijk aanzienlijke schade, met name met voldoende belangrijke negatieve gevolgen voor de fysieke of psychologische gezondheid of voor financiële belangen, zal optreden, is bijzonder gevaarlijk en moet daarom worden verboden. Dergelijke AI-systemen maken gebruik van subliminale componenten zoals audio-, beeld- en videostimuli die personen niet kunnen waarnemen, omdat deze stimuli verder gaan dan de menselijke perceptie, of andere manipulatieve of bedrieglijke technieken die de autonomie, besluitvorming of vrije keuze van personen ondermijnen of beperken op wijzen waarvan mensen zich van deze technieken niet bewust zijn of waarbij, zelfs als ze zich er bewust van zijn, ze nog steeds misleid kunnen worden of hen niet kunnen beheersen of weerstaan. Dit kan bijvoorbeeld worden vergemakkelijkt door machine-hersens-interfaces of virtuele realiteit, aangezien zij een hogere mate van controle mogelijk maken over de stimuli die aan personen worden gepresenteerd, voor zover zij hun gedrag wezenlijk kunnen verstoren op een aanzienlijk schadelijke manier. Daarnaast kunnen AI-systemen ook kwetsbaarheden uitbuiten van een persoon of een specifieke groep personen als gevolg van hun leeftijd, handicap in de zin van Richtlijn (EU) 2019/882 van het Europees Parlement en de Raad¹⁶ of een specifieke sociale of economische situatie waardoor deze personen waarschijnlijk kwetsbaarder zullen zijn voor uitbuiting, zoals personen die in extreme armoede leven of personen die tot een etnische of religieuze minderheid behoren.

¹⁶ Richtlijn (EU) 2019/882 van het Europees Parlement en de Raad van 17 april 2019 betreffende de toegankelijkheidsvoorschriften voor producten en diensten (PB L 151 van 7.6.2019, blz. 70).

Dergelijke AI-systemen kunnen in de handel worden gebracht, in gebruik worden gesteld of worden gebruikt met als doel of als gevolg dat het gedrag van een persoon wezenlijk wordt verstoord op een manier die deze persoon, een andere persoon of groepen personen aanzienlijke schade berokkent of redelijkerwijs dreigt te berokkenen, met inbegrip van schade die in de loop der tijd erger kan worden, en moeten daarom worden verboden. Er kan worden aangenomen dat er geen sprake is van een intentie om gedrag te verstoren wanneer de verstoring het gevolg is van factoren buiten het AI-systeem waarop de aanbieder of de gebruiksverantwoordelijke geen invloed heeft, namelijk factoren die redelijkerwijs niet te voorzien zijn en die de aanbieder of de gebruiksverantwoordelijke van het AI-systeem bijgevolg niet kan beperken. In ieder geval is het niet vereist dat de aanbieder of de gebruiksverantwoordelijke de intentie heeft aanzienlijke schade te berokkenen, op voorwaarde dat deze schade het gevolg is van op AI gebaseerde manipulatieve of uitbuitingspraktijken. De verbodsbepalingen voor dergelijke AI-praktijken vormen een aanvulling op de bepalingen van Richtlijn 2005/29/EG van het Europees Parlement en de Raad¹⁷, met name die bepalingen waarin is vastgesteld dat oneerlijke handelspraktijken die tot economische of financiële schade voor consumenten leiden onder alle omstandigheden verboden zijn, ongeacht of zij via AI-systemen of anderszins tot stand worden gebracht. Het verbod op manipulatie- en uitbuitingspraktijken in deze verordening mag geen afbreuk doen aan rechtmatige praktijken in het kader van medische behandelingen, zoals psychologische behandeling van een psychische aandoening of lichamelijke revalidatie, wanneer die praktijken worden uitgevoerd overeenkomstig de toepasselijke medische normen en wetgeving, bijvoorbeeld met uitdrukkelijke toestemming van de natuurlijke personen of hun wettelijke vertegenwoordigers. Bovendien mogen gangbare en legitieme handelspraktijken, bijvoorbeeld in de reclamesector, die in overeenstemming zijn met het toepasselijke recht op zich niet worden beschouwd als schadelijke manipulatieve op AI gebaseerde praktijken.

¹⁷ Richtlijn 2005/29/EG van het Europees Parlement en de Raad van 11 mei 2005 betreffende oneerlijke handelspraktijken van ondernemingen jegens consumenten op de interne markt en tot wijziging van Richtlijn 84/450/EEG van de Raad, Richtlijnen 97/7/EG, 98/27/EG en 2002/65/EG van het Europees Parlement en de Raad en van Verordening (EG) nr. 2006/2004 van het Europees Parlement en de Raad (“Richtlijn oneerlijke handelspraktijken”) (PB L 149 van 11.6.2005, blz. 22).

- (30) Systemen voor biometrische categorisering die gebaseerd zijn op biometrische gegevens van natuurlijke personen, zoals het gezicht of vingerafdrukken, om de politieke opvattingen, het lidmaatschap van een vakbond, religieuze of levensbeschouwelijke overtuigingen, ras, seksleven of seksuele gerichtheid van een persoon af te leiden of te infereren, moeten worden verboden. Dat verbod mag geen betrekking hebben op het rechtmatig labelen, filteren of categoriseren van reeksen biometrische gegevens die in overeenstemming met het Unierecht of het nationale recht met betrekking tot biometrische gegevens zijn verkregen, zoals het sorteren van beelden op basis van haar- of oogkleur, die bijvoorbeeld op het gebied van rechtshandhaving kunnen worden gebruikt.
- (31) AI-systemen die door publieke of door private actoren worden gebruikt om een beoordeling van natuurlijke personen (“social scoring”) uit te voeren, kunnen discriminerende resultaten en de uitsluiting van bepaalde groepen tot gevolg hebben. Deze systemen kunnen een schending inhouden van het recht op waardigheid en non-discriminatie en van waarden als gelijkheid en rechtvaardigheid. Dergelijke AI-systemen beoordelen of classificeren natuurlijke personen of groepen natuurlijke personen op basis van meerdere datapunten met betrekking tot hun sociale gedrag in meerdere contexten of op basis van bekende, afgeleide of voorspelde persoonlijke of persoonlijkheidskenmerken gedurende een bepaalde periode. De sociale score die dergelijke AI-systemen opleveren, kan leiden tot een nadelige of ongunstige behandeling van natuurlijke personen of hele groepen natuurlijke personen in sociale contexten die geen verband houden met de context waarin de data oorspronkelijk zijn gegenereerd of verzameld, of tot een nadelige behandeling die onevenredig of ongerechtvaardigd is in verhouding tot de ernst van het sociale gedrag. AI-systemen die dergelijke onaanvaardbare scoringpraktijken met zich meebrengen en tot dergelijke nadelige of ongunstige resultaten leiden, moeten daarom worden verboden. Dat verbod mag geen afbreuk doen aan wettige praktijken voor de evaluatie van natuurlijke personen die worden verricht voor een specifieke doeleinde in overeenstemming met het Unierecht en het nationale recht.

- (32) Het gebruik van AI-systemen voor biometrische identificatie op afstand in real time van natuurlijke personen in openbare ruimten voor rechtshandavingsdoeleinden wordt als bijzonder ingrijpend beschouwd voor de rechten en vrijheden van de betrokkenen, in die mate dat het de persoonlijke levenssfeer van een groot deel van de bevolking kan aantasten, een gevoel van voortdurende bewaking kan oproepen en indirect de uitoefening van de vrijheid van vergadering en andere grondrechten kan ontmoedigen. Technische onnauwkeurigheden van AI-systemen voor biometrische identificatie op afstand van natuurlijke personen kunnen tot vertekende resultaten en discriminerende effecten leiden. Dergelijke mogelijke vertekende resultaten en discriminerende effecten zijn met name relevant met betrekking tot leeftijd, etniciteit, ras, geslacht of handicap. Bovendien houden het directe karakter van de gevolgen en de beperkte mogelijkheden voor verdere controles of correcties met betrekking tot het gebruik van dergelijke realsystemen, verhoogde risico's in voor de rechten en vrijheden van de betrokken personen in de context van rechtshandavingsactiviteiten of wanneer die personen van de rechtshandavingsactiviteiten gevolgen ondervinden.

- (33) Het gebruik van dergelijke systemen voor rechtshandavingsdoeleinden moet derhalve worden verboden, behalve in limitatief opgesomde en nauwkeurig omschreven situaties, waarin het gebruik strikt noodzakelijk is om een zwaarwegend algemeen belang te dienen, dat zwaarder weegt dan de risico's. Die situaties hebben betrekking op de zoektocht naar bepaalde slachtoffers van misdrijven, waaronder vermiste personen; bepaalde bedreigingen ten aanzien van het leven of de fysieke veiligheid van natuurlijke personen of van een terroristische aanslag; en de lokalisatie of identificatie van daders of verdachten van de in een bijlage bij deze verordening genoemde strafbare feiten, indien die strafbare feiten in de betrokken lidstaat strafbaar zijn gesteld met een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel met een maximumduur van ten minste vier jaar en zoals zij zijn gedefinieerd in het recht van die lidstaat. Een dergelijke drempel voor de vrijheidsstraf of de tot vrijheidsbeneming strekkende maatregel overeenkomstig het nationale recht helpt erop toe te zien dat het strafbare feit ernstig genoeg is om het gebruik van systemen voor biometrische identificatie op afstand in real time te rechtvaardigen. De in een bijlage bij deze verordening genoemde strafbare feiten zijn gebaseerd op de 32 in Kaderbesluit 2002/584/JBZ van de Raad¹⁸ genoemde strafbare feiten, ermee rekening houdend dat sommige van die strafbare feiten in de praktijk waarschijnlijk relevanter zijn dan andere, aangezien het gebruik van biometrische identificatie op afstand in real time naar verwachting in zeer uiteenlopende mate noodzakelijk en evenredig zou kunnen zijn voor de praktische uitvoering van de lokalisatie of identificatie van een dader of verdachte van de verschillende opgesomde strafbare feiten, gelet op de te verwachten verschillen in ernst, waarschijnlijkheid en omvang van de schade of de mogelijke negatieve gevolgen.

¹⁸ Kaderbesluit 2002/584/JBZ van de Raad van 13 juni 2002 betreffende het Europees aanhoudingsbevel en de procedures van overlevering tussen de lidstaten (PB L 190 van 18.7.2002, blz. 1).

Een imminente dreiging voor het leven of de fysieke veiligheid van natuurlijke personen kan ook het gevolg zijn van een ernstige verstoring van kritieke infrastructuur, zoals gedefinieerd in artikel 2, punt 4), van Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad¹⁹, wanneer de verstoring of vernietiging van dergelijke kritieke infrastructuur zou leiden tot een imminente dreiging voor het leven of de fysieke veiligheid van een persoon, onder meer door ernstige schade aan de levering van basisvoorzieningen aan de bevolking of aan de uitoefening van de kernfunctie van de staat. Daarnaast moet deze verordening de rechtshandhavingsinstanties en de grenstoezichts-, immigratie- of asielautoriteiten in staat stellen identiteitscontroles uit te voeren in aanwezigheid van de betrokken persoon overeenkomstig de voorwaarden die in het Unierecht en het nationale recht voor dergelijke controles zijn vastgelegd. Met name moeten die autoriteiten informatiesystemen kunnen gebruiken in overeenstemming met het Unierecht of het nationale recht om personen te identificeren die tijdens een identiteitscontrole weigeren te worden geïdentificeerd of niet in staat zijn hun identiteit bekend te maken of te bewijzen, zonder dat zij door deze verordening verplicht worden om voorafgaande toestemming te verkrijgen. Het kan hierbij bijvoorbeeld gaan om een persoon die betrokken is bij een misdrijf of iemand die als gevolg van een ongeval of een medische aandoening niet bereid of in staat is zijn identiteit bekend te maken aan rechtshandhavingsinstanties.

¹⁹ Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PB L 333 van 27.12.2022, blz. 164).

- (34) Om ervoor te zorgen dat dergelijke systemen op een verantwoorde en evenredige wijze worden gebruikt, is het ook van belang om vast te stellen dat in elk van die limitatief opgesomde en nauwkeurig omschreven situaties bepaalde elementen in aanmerking moeten worden genomen, met name wat betreft de aard van de situatie die aan het verzoek ten grondslag ligt en de gevolgen van het gebruik voor de rechten en vrijheden van alle betrokken personen, alsook de waarborgen en voorwaarden waaraan het gebruik is onderworpen. Daarnaast mag het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op rechtshandhaving alleen worden ingezet om de identiteit van de specifiek beoogde natuurlijke persoon te bevestigen en moet het worden beperkt tot wat strikt noodzakelijk qua duur en geografische en personele reikwijdte, met name rekening houdend met het bewijs of de aanwijzingen met betrekking tot de dreigingen, de slachtoffers of de dader. Het gebruik van het systeem voor biometrische identificatie op afstand in real time in openbare ruimten mag alleen worden toegestaan indien de betrokken rechtshandhavingsinstantie een in deze verordening bedoelde effectbeoordeling op het gebied van de grondrechten heeft voltooid en, tenzij anders bepaald in deze verordening, het systeem in de databank heeft geregistreerd zoals vastgelegd in deze verordening. De referentiedatabank van personen moet geschikt zijn voor elk gebruik in elk van de bovenvermelde situaties.

- (35) Voor elk gebruik van een systeem voor biometrische identificatie op afstand in real time in openbare ruimten voor rechtshandavingsdoeleinden moet uitdrukkelijke en specifieke toestemming vereist zijn van een gerechtelijke instantie of van een onafhankelijke administratieve instantie van een lidstaat, met bindende beslissingsbevoegdheid. Deze toestemming moet in beginsel worden verkregen voordat het AI-systeem voor de identificatie van een of meer personen wordt gebruikt. Uitzonderingen op deze regel moeten worden toegestaan in naar behoren gemotiveerde dringende situaties, namelijk in situaties waarin het wegens de noodzaak om het betrokken AI-systeem te gebruiken, feitelijk en objectief onmogelijk is om vóór het begin van het gebruik toestemming te verkrijgen. In dergelijke dringende situaties moet het gebruik van het AI-systeem worden beperkt tot het absoluut noodzakelijke minimum en onderworpen zijn aan passende waarborgen en voorwaarden, zoals bepaald in de nationale wetgeving en door de rechtshandavingsinstantie zelf vastgesteld in de context van elk afzonderlijk dringend gebruik. In dergelijke situaties moet de rechtshandavingsinstantie onverwijld en uiterlijk binnen 24 uur om dergelijke toestemming verzoeken, met opgave van de redenen waarom zij niet eerder een verzoek daartoe heeft kunnen indienen. Indien een dergelijke toestemming wordt geweigerd, moet het gebruik van systemen voor biometrische identificatie in real time waarop dat verzoek betrekking heeft, met onmiddellijke ingang worden stopgezet en moeten alle gegevens met betrekking tot dat gebruik worden verwijderd en gewist. Onder dergelijke gegevens wordt verstaan: inputdata die rechtstreeks door een AI-systeem zijn verkregen tijdens het gebruik van een dergelijk systeem, alsook de resultaten en output van het gebruik in verband met dat verzoek. Daaronder mag niet worden verstaan: input die rechtmatig is verkregen overeenkomstig een ander Unierecht of nationaal recht. In geen geval mag een besluit dat nadelige rechtsgevolgen heeft voor een persoon uitsluitend worden genomen op basis van de output van het systeem voor biometrische identificatie op afstand.

- (36) Om hun taken overeenkomstig de eisen van deze verordening en de nationale regels uit te voeren, moeten de betrokken markttoezichtautoriteit en de nationale gegevensbeschermingsautoriteit in kennis worden gesteld van elk gebruik van het systeem voor biometrische identificatie in real time. De markttoezicht-autoriteiten en de nationale gegevensbeschermingsautoriteiten die in kennis zijn gesteld, moeten bij de Commissie een jaarverslag indienen over het gebruik van systemen voor biometrische identificatie in real time.
- (37) Voorts moet binnen het door deze verordening gestelde limitatieve kader worden vastgelegd dat een dergelijk gebruik op het grondgebied van een lidstaat overeenkomstig deze verordening alleen mogelijk mag zijn indien en voor zover de betrokken lidstaat heeft besloten om in zijn specifieke regels van nationaal recht uitdrukkelijk te voorzien in de mogelijkheid om een dergelijk gebruik toe te staan. Bijgevolg staat het de lidstaten uit hoofde van deze verordening vrij in het geheel niet in een dergelijke mogelijkheid te voorzien, dan wel slechts in een dergelijke mogelijkheid te voorzien voor een aantal van de in deze verordening genoemde doelstellingen die het toestaan van een dergelijk gebruik rechtvaardigen. Dergelijke nationale regels moeten binnen dertig dagen na de vaststelling ervan ter kennis van de Commissie worden gebracht.

- (38) Het gebruik van AI-systemen voor biometrische identificatie op afstand in real time van natuurlijke personen in openbare ruimten voor rechtshandavingsdoeleinden brengt noodzakelijkerwijs de verwerking van biometrische gegevens met zich mee. De regels in deze verordening die, met inachtneming van bepaalde uitzonderingen, een dergelijk gebruik verbieden en die gebaseerd zijn op artikel 16 VWEU, moeten als *lex specialis* gelden ten aanzien van de regels inzake de verwerking van biometrische gegevens in artikel 10 van Richtlijn (EU) 2016/680, waardoor een dergelijk gebruik en de bijbehorende verwerking van biometrische gegevens limitatief worden geregeld. Daarom mogen een dergelijk gebruik en een dergelijke verwerking alleen mogelijk zijn voor zover zij verenigbaar zijn met het bij deze verordening vastgestelde kader, zonder dat er buiten dat kader ruimte is voor de bevoegde autoriteiten om, wanneer zij optreden met het oog op de rechtshandhaving, dergelijke systemen te gebruiken en dergelijke gegevens in verband daarmee te verwerken om de in artikel 10 van Richtlijn (EU) 2016/680 genoemde redenen. In die context is deze verordening niet bedoeld om de rechtsgrondslag te bieden voor de verwerking van persoonsgegevens op grond van artikel 8 van Richtlijn (EU) 2016/680. Het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten voor andere doeleinden dan rechtshandhaving, ook door bevoegde autoriteiten, mag echter niet worden opgenomen in het specifieke kader met betrekking tot dergelijk gebruik voor rechtshandavingsdoeleinden dat bij deze verordening wordt vastgesteld. Dergelijk gebruik voor andere doeleinden dan rechtshandhaving is derhalve niet onderworpen aan het vereiste van toestemming uit hoofde van deze verordening en de toepasselijke specifieke regels van nationaal recht die aan die toestemming uitvoering kunnen geven.

- (39) Elke verwerking van biometrische gegevens en andere persoonsgegevens in het kader van het gebruik van AI-systemen voor biometrische identificatie, die geen verband houdt met het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten voor rechtshandavingsdoeleinden zoals geregeld in deze verordening, moet blijven voldoen aan alle eisen die voortvloeien uit artikel 10 van Richtlijn (EU) 2016/680. Voor andere doeleinden dan rechtshandhaving verbieden artikel 9, lid 1, van Verordening (EU) 2016/679 en artikel 10, lid 1, van Verordening (EU) 2018/1725 de verwerking van biometrische gegevens, met inachtneming van beperkte uitzonderingen zoals bepaald in die artikelen. Bij de toepassing van artikel 9, lid 1, van Verordening (EU) 2016/679 is het gebruik van biometrische identificatie op afstand voor andere doeleinden dan rechtshandhaving reeds onderworpen aan verbodsbesluiten van nationale gegevensbeschermingsautoriteiten.

- (40) Overeenkomstig artikel 6 bis van Protocol nr. 21 betreffende de positie van het Verenigd Koninkrijk en Ierland ten aanzien van de ruimte van vrijheid, veiligheid en recht, gehecht aan het VEU en het VWEU, is Ierland niet gebonden door de regels die zijn vastgelegd in artikel 5, lid 1, eerste alinea, punt g), voor zover dit van toepassing is op het gebruik van systemen voor biometrische categorisering voor activiteiten op het gebied van politieke samenwerking en justitiële samenwerking in strafzaken, artikel 5, lid 1, eerste alinea, punt d), voor zover het van toepassing is op het gebruik van onder die bepaling vallende AI-systemen, artikel 5, lid 1, eerste alinea, punt h), artikel 5, leden 2 tot en met 6, en artikel 26, lid 10, van deze verordening, en die zijn vastgesteld op basis van artikel 16 VWEU in verband met de verwerking van persoonsgegevens door de lidstaten bij de uitvoering van activiteiten binnen het toepassingsgebied van hoofdstuk 4 of 5 van titel V van het derde deel van het VWEU, wanneer Ierland niet gebonden is door de regels betreffende de vormen van justitiële samenwerking in strafzaken of van politieke samenwerking in het kader waarvan de op grond van artikel 16 VWEU vastgestelde bepalingen moeten worden nageleefd.

- (41) Overeenkomstig de artikelen 2 en 2 bis van Protocol nr. 22 betreffende de positie van Denemarken, gehecht aan het VEU en het VWEU, zijn de regels in artikel 5, lid 1, eerste alinea, punt g), voor zover dit van toepassing is op het gebruik van systemen voor biometrische categorisering voor activiteiten op het gebied van politieke samenwerking en justitiële samenwerking in strafzaken, artikel 5, lid 1, eerste alinea, punt d), voor zover het van toepassing is op het gebruik van onder die bepaling vallende AI-systemen, artikel 5, lid 1, eerste alinea, punt h), artikel 5, leden 2 tot en met 6, en artikel 26, lid 10, van deze verordening, die zijn vastgesteld op basis van artikel 16 VWEU, in verband met de verwerking van persoonsgegevens door de lidstaten bij de uitvoering van activiteiten binnen het toepassingsgebied van hoofdstuk 4 of 5 van titel V van het derde deel van het VWEU, niet bindend voor, noch van toepassing op Denemarken.

- (42) In overeenstemming met het vermoeden van onschuld moeten natuurlijke personen in de Unie altijd worden beoordeeld op hun feitelijke gedrag. Natuurlijke personen mogen nooit worden beoordeeld op basis van door AI voorspeld gedrag dat uitsluitend gebaseerd is op hun profilering, persoonlijkheidskenmerken of kenmerken, zoals nationaliteit, geboorteplaats, verblijfplaats, aantal kinderen, schuldniveau of type auto, zonder een redelijk vermoeden dat die persoon betrokken is bij een criminele activiteit op basis van objectieve, verifieerbare feiten en zonder menselijke beoordeling daarvan. Daarom moeten risicobeoordelingen die met betrekking tot natuurlijke personen worden uitgevoerd, uitsluitend op basis van profilering of beoordeling van hun persoonlijkheidskenmerken en kenmerken, om de waarschijnlijkheid dat zij strafbare feiten plegen, te beoordelen, of om te voorspellen dat er een feitelijk of potentieel strafbaar feit zal plaatsvinden, worden verboden. In elk geval heeft dat verbod geen betrekking op risicoanalyses die niet zijn gebaseerd op de profilering van natuurlijke personen of op de persoonlijkheidskenmerken en kenmerken van natuurlijke personen, zoals AI-systemen die gebruikmaken van risicoanalyses om de waarschijnlijkheid van financiële fraude door ondernemingen te beoordelen op basis van verdachte transacties, of van risicoanalyse-instrumenten om de waarschijnlijkheid van vondsten van verdovende middelen of illegale goederen door douaneautoriteiten te voorspellen, bijvoorbeeld op basis van bekende smokkelroutes.
- (43) Het in de handel brengen, het in gebruik stellen voor dat specifieke doel en het gebruiken van AI-systemen die databanken voor gezichtsherkenning creëren of uitbreiden door middel van de niet-gerichte scraping van gezichtsopnamen van het internet of CCTV-beelden, moeten worden verboden omdat dergelijke praktijken het gevoel van grootschalig toezicht vergroten en kunnen leiden tot grove schendingen van de grondrechten, waaronder het recht op privacy.

- (44) Er bestaat ernstige bezorgdheid over de wetenschappelijke basis van AI-systemen die gericht zijn op het identificeren of afleiden van emoties, met name omdat emoties sterk uiteenlopen tussen culturen en situaties, en zelfs bij één persoon. Tot de belangrijkste tekortkomingen van dergelijke systemen behoren de beperkte betrouwbaarheid, het gebrek aan specificiteit en de beperkte veralgemeenbaarheid. Daarom kunnen AI-systemen die emoties of intenties van natuurlijke personen identificeren of afleiden op basis van hun biometrische gegevens, tot discriminerende resultaten leiden en inbreuk maken op de rechten en vrijheden van de betrokken personen. Gezien de ongelijke machtsverhoudingen in de context van werk of onderwijs, in combinatie met het ingrijpende karakter van deze systemen, kunnen dergelijke systemen leiden tot een nadelige of ongunstige behandeling van bepaalde natuurlijke personen of hele groepen personen. Daarom moeten het in de handel brengen, in gebruik stellen en gebruiken van AI-systemen die bedoeld zijn om te worden gebruikt om de emotionele toestand van natuurlijke personen in situaties die verband houden met de werkplek en het onderwijs te detecteren, worden verboden. Dat verbod mag geen betrekking hebben op AI-systemen die uitsluitend om medische of veiligheidsredenen in de handel worden gebracht, zoals systemen die bedoeld zijn voor therapeutisch gebruik.
- (45) Deze verordening moet praktijken die verboden zijn uit hoofde van het Unierecht, met inbegrip van het gegevensbeschermingsrecht, het non-discriminatierecht, het recht inzake consumentenbescherming, en het mededingingsrecht, onverlet laten.

- (46) AI-systemen met een hoog risico mogen alleen in de Unie in de handel worden gebracht, in gebruik worden gesteld of worden gebruikt als zij aan bepaalde dwingende eisen voldoen. Die eisen moeten ervoor zorgen dat AI-systemen met een hoog risico die in de Unie beschikbaar zijn of waarvan de output anderszins in de Unie wordt gebruikt, geen onaanvaardbare risico's inhouden voor belangrijke publieke belangen in de Unie, zoals die door het recht van de Unie worden erkend en beschermd. Op basis van het nieuwe wetgevingskader, zoals verduidelijkt in de mededeling van de Commissie "De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU"²⁰, luidt de algemene regel dat meer dan een rechtshandeling van de harmonisatiewetgeving van de Unie, zoals de Verordeningen (EU) 2017/745²¹ en (EU) 2017/746²² van het Europees Parlement en de Raad of Richtlijn 2006/42/EG van het Europees Parlement en de Raad²³, op één product van toepassing kan zijn, aangezien het aanbieden of in gebruik stellen van het product alleen kan plaatsvinden wanneer het product voldoet aan alle toepasselijke harmonisatiewetgeving van de Unie. Om consistentie te waarborgen en onnodige administratieve lasten of kosten te vermijden, moeten aanbieders van een product dat een of meer AI-systemen met een hoog risico bevat waarop de eisen van deze verordening en van de harmonisatiewetgeving van de Unie zoals vermeld in een bijlage bij deze verordening van toepassing zijn, flexibel zijn met betrekking tot operationele beslissingen over hoe ervoor kan worden gezorgd dat een product dat een of meer AI-systemen bevat, op optimale wijze voldoet aan alle toepasselijke eisen van die harmonisatiewetgeving van de Unie. De aanmerking als AI-systeem met een hoog risico, moet worden beperkt tot systemen die aanzienlijke schadelijke gevolgen hebben voor de gezondheid, de veiligheid en de grondrechten van personen in de Unie, en daarbij moeten potentiële restricties voor de internationale handel tot een minimum worden beperkt.

²⁰ PB C 247 van 29.6.2022, blz. 1.

²¹ Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (PB L 117 van 5.5.2017, blz. 1).

²² Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176).

²³ Richtlijn 2006/42/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende machines en tot wijziging van Richtlijn 95/16/EG (PB L 157 van 9.6.2006, blz. 24).

- (47) AI-systemen kunnen nadelige gevolgen hebben voor de gezondheid en de veiligheid van personen, met name wanneer dergelijke systemen functioneren als veiligheidscomponenten van producten. Overeenkomstig de in de harmonisatiewetgeving van de Unie beoogde doelstellingen om het vrije verkeer van producten op de interne markt te vergemakkelijken en ervoor te zorgen dat alleen veilige en anderszins conforme producten hun weg naar de markt vinden, is het belangrijk dat de veiligheidsrisico's die een product in zijn geheel kan genereren door zijn digitale componenten, waaronder AI-systemen, naar behoren worden voorkomen en beperkt. Zo moeten robots die alsmaar autonoom worden, of het nu in een productieomgeving is of voor persoonlijke hulp en zorg, in staat zijn op een veilige manier te werken en hun taken uit te voeren in complexe omgevingen. Ook in de gezondheidssector, waar het belang voor leven en gezondheid bijzonder hoog is, moeten de steeds geavanceerdere diagnosesystemen en systemen ter ondersteuning van menselijke beslissingen betrouwbaar en nauwkeurig zijn.

- (48) Een bijzonder relevante factor voor de classificering van een AI-systeem als AI-systeem met een hoog risico, is de omvang van de door het AI-systeem veroorzaakte nadelige effecten op de grondrechten die door het Handvest worden beschermd. Onder die rechten zijn begrepen: het recht op menselijke waardigheid, de eerbiediging van het privéleven en van het familie- en gezinsleven, de bescherming van persoonsgegevens, de vrijheid van meningsuiting en van informatie, de vrijheid van vergadering en vereniging, het recht op non-discriminatie, het recht op onderwijs, consumentenbescherming, de rechten van werknemers, de rechten van personen met een handicap, gendergelijkheid, intellectuele-eigendomsrechten, het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, het recht op verdediging en het vermoeden van onschuld, alsook het recht op behoorlijk bestuur. Naast deze rechten moeten ook de specifieke rechten van kinderen worden benadrukt, die zijn vastgelegd in artikel 24 van het Handvest en in het Verdrag van de Verenigde Naties inzake de rechten van het kind, nader uitgewerkt in algemene opmerking nr. 25 van het VN-Comité voor de rechten van het kind met betrekking tot de digitale omgeving, waarbij telkens wordt geëist dat rekening wordt gehouden met de kwetsbaarheid van kinderen en dat zij de bescherming en zorg krijgen die nodig zijn voor hun welbevinden. Ook het grondrecht betreffende een hoog niveau van milieubescherming, dat in het Handvest is vastgelegd en in het beleid van de Unie wordt uitgevoerd, moet in aanmerking worden genomen bij de beoordeling van de ernst van de schade die een AI-systeem kan veroorzaken, onder meer met betrekking tot de gezondheid en de veiligheid van personen.

- (49) Wat betreft AI-systemen met een hoog risico die veiligheidscomponenten zijn van producten of systemen, of die zelf producten of systemen zijn die onder het toepassingsgebied vallen van Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad²⁴, Verordening (EU) nr. 167/2013 van het Europees Parlement en de Raad²⁵, Verordening (EU) nr. 168/2013 van het Europees Parlement en de Raad²⁶, Richtlijn 2014/90/EU van het Europees Parlement en de Raad²⁷, Richtlijn (EU) 2016/797 van het Europees Parlement en de Raad²⁸,

-
- ²⁴ Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72).
- ²⁵ Verordening (EU) nr. 167/2013 van het Europees Parlement en de Raad van 5 februari 2013 inzake de goedkeuring van en het markttoezicht op landbouw- en bosbouwvoertuigen (PB L 60 van 2.3.2013, blz. 1).
- ²⁶ Verordening (EU) nr. 168/2013 van het Europees Parlement en de Raad van 15 januari 2013 betreffende de goedkeuring van en het markttoezicht op twee- of driewielige voertuigen en vierwielers (PB L 60 van 2.3.2013, blz. 52).
- ²⁷ Richtlijn 2014/90/EU van het Europees Parlement en de Raad van 23 juli 2014 inzake uitrusting van zeeschepen en tot intrekking van Richtlijn 96/98/EG van de Raad (PB L 257 van 28.8.2014, blz. 146).
- ²⁸ Richtlijn (EU) 2016/797 van het Europees Parlement en de Raad van 11 mei 2016 betreffende de interoperabiliteit van het spoorwegsysteem in de Europese Unie (PB L 138 van 26.5.2016, blz. 44).

Verordening (EU) 2018/858 van het Europees Parlement en de Raad²⁹,
Verordening (EU) 2018/1139 van het Europees Parlement en de Raad³⁰, en
Verordening (EU) 2019/2144 van het Europees Parlement en de Raad³¹, moeten die
handelingen worden gewijzigd om ervoor te zorgen dat de Commissie, op basis van de
technische en regelgeving van elke sector en zonder in te grijpen in de bestaande
governance-, conformiteitsbeoordelings- en handhavingsmechanismen en autoriteiten die
daarbij zijn ingesteld, rekening houdt met de in deze verordening vastgelegde dwingende
eisen voor AI-systemen met een hoog risico wanneer zij op basis van die handelingen
desbetreffende gedelegeerde of uitvoeringshandelingen vaststelt.

-
- ²⁹ Verordening (EU) 2018/858 van het Europees Parlement en de Raad van 30 mei 2018
betreffende de goedkeuring van en het markttoezicht op motorvoertuigen en aanhangwagens
daarvan en systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn
bestemd, tot wijziging van Verordeningen (EG) nr. 715/2007 en (EG) nr. 595/2009 en tot
intrekking van Richtlijn 2007/46/EG (PB L 151 van 14.6.2018, blz. 1).
- ³⁰ Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake
gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een
Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging
van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010,
(EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees
Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004
en (EG) nr. 216/2008 van het Europees Parlement en de Raad en
Verordening (EEG) nr. 3922/91 van de Raad (PB L 212 van 22.8.2018, blz. 1).
- ³¹ Verordening (EU) 2019/2144 van het Europees Parlement en de Raad van
27 november 2019 betreffende de voorschriften voor de typegoedkeuring van
motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische
eenheden die voor dergelijke voertuigen zijn bestemd wat de algemene veiligheid ervan en
de bescherming van de inzittenden van voertuigen en kwetsbare weggebruikers betreft, tot
wijziging van Verordening (EU) 2018/858 van het Europees Parlement en de Raad en tot
intrekking van de Verordeningen (EG) nr. 78/2009, (EG) nr. 79/2009 en (EG) nr. 661/2009
van het Europees Parlement en de Raad en de Verordeningen (EG) nr. 631/2009,
(EU) nr. 406/2010, (EU) nr. 672/2010, (EU) nr. 1003/2010, (EU) nr. 1005/2010,
(EU) nr. 1008/2010, (EU) nr. 1009/2010, (EU) nr. 19/2011, (EU) nr. 109/2011,
(EU) nr. 458/2011, (EU) nr. 65/2012, (EU) nr. 130/2012, (EU) nr. 347/2012,
(EU) nr. 351/2012, (EU) nr. 1230/2012 en (EU) 2015/166 van de Commissie (PB L 325
van 16.12.2019, blz. 1).

- (50) Wat AI-systemen betreft die veiligheidscomponenten van producten zijn, of die zelf producten zijn, en die onder het toepassingsgebied van bepaalde in een bijlage bij deze verordening vermelde harmonisatiewetgeving van de Unie vallen, is het passend ze in het kader van deze verordening als AI-systemen met een hoog risico te classificeren indien het betrokken product de conformiteits-beoordelingsprocedure ondergaat bij een conformiteitsbeoordelingsinstantie op grond van die relevante harmonisatiewetgeving van de Unie. Het gaat met name om machines, speelgoed, liften, uitrusting en beveiligingssystemen bestemd voor gebruik op plaatsen waar ontploffingsgevaar kan heersen, radioapparatuur, drukapparatuur, pleziervaartuigen, kabelbaaninstallaties, gastoestellen, medische hulpmiddelen, medische hulpmiddelen voor in-vitrodiagnostiek, de automobiel- en de luchtvaartsector.
- (51) De classificatie van een AI-systeem als een AI-systeem met een hoog risico op grond van deze verordening hoeft niet te betekenen dat het product waarvan het AI-systeem de veiligheidscomponent is, of het AI-systeem zelf als product, als “een systeem met een hoog risico” wordt beschouwd volgens de criteria die zijn vastgelegd in de toepasselijke harmonisatiewetgeving van de Unie die op het product van toepassing is. Dit is met name het geval voor de Verordeningen (EU) 2017/745 en (EU) 2017/746, waarin wordt voorzien in een conformiteitsbeoordeling door een derde partij voor producten met een middelgroot risico en producten met een hoog risico.

- (52) Autonome AI-systemen, d.w.z. andere AI-systemen met een hoog risico dan die welke veiligheidscomponenten van producten zijn of die zelf producten zijn, moeten als AI-systemen met een hoog risico worden geclassificeerd indien zij, gelet op het beoogde doel, een hoog risico inhouden op schade aan de gezondheid en de veiligheid of aan de grondrechten van personen, rekening houdend met zowel de ernst van de mogelijke schade als de waarschijnlijkheid dat deze zich voordoet, en indien zij worden gebruikt op een aantal in deze verordening beschreven, specifieke en vooraf bepaalde gebieden. De identificatie van die systemen is gebaseerd op dezelfde methode en criteria die ook worden overwogen voor toekomstige wijzigingen van de lijst van AI-systemen met een hoog risico die de Commissie via gedelegeerde handelingen moet kunnen vaststellen om rekening te houden met het snelle tempo van de technologische ontwikkeling en met de mogelijke veranderingen in het gebruik van AI-systemen.

- (53) Het is ook belangrijk te verduidelijken dat er specifieke gevallen kunnen zijn waarin AI-systemen die worden gebruikt op in deze verordening beschreven, specifieke gebieden, niet leiden tot een aanzienlijk risico op schade aan de juridische belangen die op die gebieden worden beschermd, omdat zij de besluitvorming niet wezenlijk beïnvloeden of die belangen niet wezenlijk schaden. Voor de toepassing van deze verordening moet een AI-systeem dat het resultaat van de besluitvorming niet wezenlijk beïnvloedt, worden beschouwd als een AI-systeem dat geen invloed heeft op de inhoud, en daarmee op het resultaat, van de menselijke of geautomatiseerde besluitvorming. Er kan sprake zijn van een AI-systeem dat het resultaat van de besluitvorming niet wezenlijk beïnvloedt, indien aan een of meer van de volgende voorwaarden is voldaan. De eerste voorwaarde luidt dat het AI-systeem bedoeld moet zijn om een enge procedurele taak uit te voeren, zoals een AI-systeem dat ongestructureerde data omzet in gestructureerde data, een AI-systeem dat binnenkomende documenten classificeert in categorieën of een AI-systeem dat wordt gebruikt om binnen een groot aantal aanvragen dubbels op te sporen. Dergelijke taken zijn dermate specifiek en beperkt dat zij slechts beperkte risico's met zich meebrengen, die niet toenemen door gebruik van een AI-systeem in een context die in een bijlage bij deze verordening als gebruik met een hoog risico is opgenomen. De tweede voorwaarde is dat de door het AI-systeem uitgevoerde taak bedoeld moet zijn om het resultaat te verbeteren van een eerder voltooide menselijke activiteit die relevant kan zijn in voor de in een lijst in een bijlage bij deze verordening vermelde gevallen van hoog-risicogebruik. Die kenmerken in beschouwing genomen, voegt het AI-systeem slechts een extra laag toe aan een menselijke activiteit, en houdt dit bijgevolg een lager risico in. Dit is bijvoorbeeld het geval voor AI-systemen die bedoeld zijn om de taal van eerder opgestelde documenten te verbeteren, bijvoorbeeld met betrekking tot professionele toon of academische stijl, of door een tekst af te stemmen op een bepaalde merkboodschap. Als derde voorwaarde geldt dat het AI-systeem bedoeld moet zijn om besluitvormingspatronen of afwijkingen van eerdere besluitvormingspatronen op te sporen.

Het risico zou in dergelijke gevallen lager liggen omdat het AI-systeem wordt gebruikt na een eerder afgeronde menselijke beoordeling en het niet de bedoeling is dat het AI-systeem deze vervangt of wijzigt zonder gedegen menselijke toetsing. Dergelijke AI-systemen omvatten bijvoorbeeld systemen die, aan de hand van een bepaald beoordelingspatroon van een leerkracht, achteraf kunnen worden gebruikt om na te gaan of de leerkracht mogelijk van dat patroon is afgeweken, en zo mogelijke inconsistenties of anomalieën te signaleren. De vierde voorwaarde houdt in dat het AI-systeem bedoeld moet zijn om een taak uit te voeren die slechts dient ter voorbereiding van een beoordeling die relevant is voor de in een bijlage bij deze verordening vermelde AI-systemen, waardoor het mogelijke effect van de output van het systeem een zeer laag risico inhoudt voor de beoordeling die erop volgt. Daarbij kan het onder meer gaan over slimme oplossingen voor bestandsbeheer, waaronder verschillende functies zoals indexerend, opzoeking, tekst- en spraakverwerking of het koppelen van gegevens aan andere gegevensbronnen, of AI-systemen die worden gebruikt voor de vertaling van brondocumenten. In elk geval moeten AI-systemen die worden gebruikt in een bijlage bij deze verordening vermelde gevallen van gebruik met een hoog risico worden geacht een aanzienlijk risico te vormen op schade aan de gezondheid, veiligheid of grondrechten indien het AI-systeem profilering inhoudt in de zin van artikel 4, punt 4), van Verordening (EU) 2016/679 of artikel 3, punt 4), van Richtlijn (EU) 2016/680 of artikel 3, punt 5), van Verordening (EU) 2018/1725. Om de traceerbaarheid en transparantie te waarborgen, moet een aanbieder die op basis van de hierboven vermelde voorwaarden van mening is dat een AI-systeem geen hoog risico vormt, documentatie van de beoordeling opstellen voordat dat systeem in de handel wordt gebracht of in gebruik wordt gesteld, en moet hij deze documentatie op verzoek aan de nationale bevoegde autoriteiten verstrekken. Een dergelijke aanbieder moet worden verplicht het AI-systeem te registreren in de EU-databank die bij deze verordening wordt opgezet. Met het oog op het verstrekken van verdere richtsnoeren voor de praktische uitvoering van de voorwaarden waaronder de in een bijlage bij deze verordening vermelde AI-systemen bij wijze van uitzondering geen hoog risico vormen, moet de Commissie, na raadpleging van de AI-board, richtsnoeren verstrekken waarin die praktische uitvoering wordt uiteengezet, aangevuld met een uitgebreide lijst van praktische voorbeelden van gebruiksgevallen van AI-systemen met een hoog risico en van gebruiksgevallen van AI-systemen zonder hoog risico.

- (54) Aangezien biometrische gegevens een bijzondere categorie persoonsgegevens vormen, is het passend verschillende gevallen van kritiek gebruik van biometrische systemen te classificeren als gebruik met een hoog risico, voor zover het gebruik is toegestaan op grond van het toepasselijke Unierecht en nationale recht. Technische onnauwkeurigheden van AI-systemen voor de biometrische identificatie op afstand van natuurlijke personen kunnen tot vertekende resultaten en discriminerende effecten leiden. Het risico op dergelijke vertekende resultaten en discriminerende effecten is met name relevant wanneer zij betrekking hebben op leeftijd, etniciteit, ras, geslacht of handicap. Systemen voor biometrische identificatie op afstand moeten daarom worden geclassificeerd als systemen met een hoog risico, gezien de risico's die zij met zich meebrengen. Een dergelijke classificatie geldt niet voor AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie, met inbegrip van authenticatie, met als enige doel te bevestigen dat een specifieke natuurlijke persoon daadwerkelijk de persoon is die die persoon beweert te zijn, en de identiteit van een natuurlijke persoon te bevestigen met als enige doel toegang te verschaffen tot een dienst, een apparaat te ontgrendelen of beveiligde toegang te verschaffen tot een locatie. Daarnaast moeten AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische categorisering op basis van krachtens artikel 9, lid 1, van Verordening (EU) 2016/679 beschermde gevoelige eigenschappen of kenmerken op basis van biometrische gegevens, voor zover deze niet verboden zijn op grond van deze verordening, en systemen voor het herkennen van emoties die niet verboden zijn op grond van deze verordening, worden geclassificeerd als systemen met een hoog risico. Biometrische systemen die uitsluitend bedoeld zijn om te worden gebruikt om cyberbeveiligings- en persoonsgegevensbeschermingsmaatregelen mogelijk te maken, mogen niet als AI-systemen met een hoog risico worden beschouwd.

- (55) Met betrekking tot het beheer en de exploitatie van kritieke infrastructuur is het passend om AI-systemen die bedoeld zijn om te worden gebruikt als veiligheidscomponent bij het beheer en de exploitatie van kritieke digitale infrastructuur als opgenomen in bijlage I, punt 8), van Richtlijn (EU) 2022/2557, wegverkeer en de levering van water, gas, verwarming en elektriciteit, te classificeren als systemen met een hoog risico, aangezien het falen of gebrekkig functioneren hiervan een grootschalig risico kan opleveren voor het leven en de gezondheid van personen en kan leiden tot aanzienlijke verstoringen van de normale beoefening van sociale en economische activiteiten. Veiligheidscomponenten van kritieke infrastructuur, waaronder kritieke digitale infrastructuur, zijn systemen die worden gebruikt om de fysieke integriteit van kritieke infrastructuur of de gezondheid en veiligheid van personen en eigendommen rechtstreeks te beschermen, maar die niet noodzakelijk zijn voor de werking van het systeem. Het falen of gebrekkig functioneren van dergelijke componenten kan direct leiden tot risico's voor de fysieke integriteit van kritieke infrastructuur en bijgevolg tot risico's voor de gezondheid en veiligheid van personen en eigendommen. Componenten die uitsluitend voor cyberbeveiligingsdoeleinden zijn bestemd, mogen niet als veiligheidscomponenten worden aangemerkt. Voorbeelden van veiligheidscomponenten van dergelijke kritieke infrastructuur zijn systemen voor de monitoring van waterdruk of brandalarminstallaties in centra voor cloud computing.

- (56) Het inzetten van AI-systemen in het onderwijs is belangrijk om digitaal onderwijs en digitale opleidingen van hoge kwaliteit te bevorderen en om alle lerenden en leerkrachten in staat te stellen de nodige digitale vaardigheden en competenties te verwerven en te delen, met inbegrip van mediageletterdheid, en kritisch denken, om actief deel te nemen aan de economie, de samenleving en democratische processen. AI-systemen die in het onderwijs of voor beroepsopleidingen worden gebruikt, met name voor het bepalen van toegang of toelating, voor het toewijzen van personen aan instellingen voor onderwijs of beroepsopleidingen of programma's op alle niveaus, voor het evalueren van leerresultaten van personen, voor de beoordeling van het passende onderwijsniveau voor een persoon en het uitoefenen van wezenlijke invloed op het niveau van onderwijs en opleiding dat aan die persoon zal worden verstrekt of waartoe die persoon toegang zal kunnen krijgen, of voor het monitoren en opsporen van ongeoorloofd gedrag van studenten tijdens tests, moeten echter als AI-systemen met een hoog risico worden geclassificeerd, aangezien ze bepalend kunnen zijn voor de onderwijs- en beroepsloopbaan van die persoon en derhalve invloed kunnen hebben op zijn vermogen om in zijn levensonderhoud te voorzien. Wanneer dergelijke systemen op ondeugdelijke wijze zijn ontworpen en worden gebruikt, kunnen zij bijzonder ingrijpend zijn en in strijd zijn met het recht op onderwijs en opleiding, alsook met het recht niet te worden gediscrimineerd, en kunnen historische patronen van discriminatie in stand worden gehouden, bijvoorbeeld ten nadele van vrouwen, bepaalde leeftijdsgroepen, personen met een handicap of personen met een bepaalde raciale of etnische afkomst of seksuele gerichtheid.

- (57) AI-systemen die worden gebruikt op het gebied van werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid, met name voor de werving en selectie van personen, voor het nemen van besluiten die van invloed zijn op de voorwaarden van arbeidsgerelateerde betrekkingen, de bevordering en beëindiging van arbeidsgerelateerde contractuele betrekkingen, voor het toewijzen van taken op basis van individueel gedrag of persoonlijke eigenschappen of kenmerken, en voor monitoring of evaluatie van personen in arbeidsgerelateerde contractuele betrekkingen, moeten ook als systemen met een hoog risico worden geclassificeerd, aangezien deze systemen aanzienlijke gevolgen kunnen hebben voor de toekomstige carrièrekansen en het levensonderhoud van deze personen, alsook voor de rechten van werknemers. Relevante arbeidsgerelateerde contractuele betrekkingen moeten, op betekenisvolle wijze, werknemers en personen omvatten die via platforms diensten verlenen, zoals bedoeld in het werkprogramma van de Commissie voor 2021. Dergelijke systemen kunnen er in het wervingsproces en bij de evaluatie, de promotie of het behoud van personen in arbeidsgerelateerde contractuele betrekkingen toe leiden dat historische patronen van discriminatie blijven bestaan, bijvoorbeeld ten aanzien van vrouwen, bepaalde leeftijdsgroepen, personen met een handicap of personen met een bepaalde raciale of etnische afkomst of seksuele gerichtheid. AI-systemen die worden gebruikt om de prestaties en het gedrag van deze personen te monitoren, kunnen ook afbreuk doen aan hun grondrechten inzake gegevensbescherming en privacy.

- (58) Een ander gebied waarop het gebruik van AI-systemen bijzondere aandacht verdient, is de toegang tot en het gebruik van bepaalde essentiële particuliere en openbare diensten en uitkeringen die noodzakelijk zijn voor de volledige deelname van personen aan de samenleving of voor het verbeteren van de levensstandaard. Met name natuurlijke personen die essentiële overheidsuitkeringen en -diensten van overheidsinstanties aanvragen of ontvangen, namelijk gezondheidszorg, socialezekerheidsuitkeringen, sociale diensten die bescherming bieden in gevallen zoals moederschap, ziekte, arbeidsongevallen, afhankelijkheid of ouderdom en verlies van werkgelegenheid en sociale bijstand en bijstand voor huisvesting, zijn doorgaans afhankelijk van deze uitkeringen en diensten en bevinden zich in een kwetsbare positie ten opzichte van de bevoegde autoriteiten. Wanneer AI-systemen worden gebruikt om te bepalen of dergelijke uitkeringen en diensten moeten worden verleend, geweigerd, beperkt, ingetrokken of teruggevorderd door de instanties, alsook of begunstigden daadwerkelijk recht hebben op dergelijke uitkeringen of diensten, kunnen deze systemen aanzienlijke effecten hebben op het levensonderhoud van personen en in strijd zijn met hun grondrechten, zoals het recht op sociale bescherming, non-discriminatie, menselijke waardigheid of een doeltreffende voorziening in rechte, en moeten zij derhalve als AI-systemen met een hoog risico worden geclassificeerd. Deze verordening mag echter niet leiden tot een belemmering van de ontwikkeling en het gebruik van innovatieve benaderingen bij de overheid, die baat zou hebben bij een breder gebruik van conforme en veilige AI-systemen, mits deze systemen geen hoog risico met zich meebrengen voor rechtspersonen en natuurlijke personen.

Voorts moeten AI-systemen die worden gebruikt om de kredietscore of de kredietwaardigheid van natuurlijke personen te evalueren, worden geëvalueerd als AI-systemen met een hoog risico, aangezien zij bepalend zijn voor de toegang van deze personen tot financiële middelen of essentiële diensten zoals huisvesting, elektriciteit en telecommunicatiediensten. AI-systemen die voor dergelijke doeleinden worden gebruikt, kunnen leiden tot de discriminatie van personen of groepen, en historische patronen van discriminatie in stand houden, bijvoorbeeld op basis van raciale of etnische afkomst, gender, handicap, leeftijd of seksuele gerichtheid, of leiden tot nieuwe soorten discriminerende effecten. AI-systemen waarin het Unierecht voorziet voor het opsporen van fraude bij het aanbieden van financiële diensten en voor prudentiële doeleinden om de kapitaalvereisten van kredietinstellingen en verzekeringsondernemingen te berekenen, mogen echter niet worden beschouwd als AI-systemen met een hoog risico uit hoofde van deze verordening. Daarnaast kunnen AI-systemen die bedoeld zijn om te worden gebruikt voor risicobeoordeling en prijsstelling met betrekking tot natuurlijke personen voor gezondheids- en levensverzekeringen ook aanzienlijke gevolgen hebben voor het levensonderhoud van personen en kunnen zij, indien zij niet naar behoren zijn ontworpen, ontwikkeld en gebruikt, inbreuk maken op hun grondrechten en ernstige gevolgen hebben voor het leven en de gezondheid van mensen, waaronder financiële uitsluiting en discriminatie. Tot slot moeten AI-systemen die worden gebruikt voor het evalueren en classificeren van noodoproepen van natuurlijke personen of om hulpdiensten, met inbegrip van politiediensten, brandweer en medische hulp, uit te sturen of hierbij voorrang te bepalen, alsook systemen voor de triage van patiënten bij dringende medische zorg, ook worden geëvalueerd als systemen met een hoog risico, omdat zij besluiten nemen in zeer kritieke situaties voor het leven en de gezondheid van personen en hun eigendom.

- (59) Gezien hun rol en verantwoordelijkheid worden maatregelen van rechtshandavingsinstanties waarbij bepaalde toepassingen van AI-systemen worden gebruikt, gekenmerkt door een aanzienlijke mate van machtsverschillen en kunnen deze leiden tot de controle, de arrestatie of de vrijheidsberoving van natuurlijke personen, alsook tot andere negatieve effecten voor de grondrechten die door het Handvest worden gewaarborgd. Met name wanneer het AI-systeem niet is getraind met kwalitatief hoogwaardige data, niet voldoet aan toereikende eisen wat betreft de prestaties, de nauwkeurigheid of robuustheid ervan of niet goed is ontworpen en getest voordat het in de handel is gebracht of anderszins in gebruik is gesteld, kan het personen op discriminerende wijze of anderszins onjuiste of onrechtvaardige wijze aanduiden. Bovendien kan de uitoefening van belangrijke procedurele grondrechten, zoals het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht, evenals de rechten van de verdediging en het vermoeden van onschuld, worden belemmerd, met name wanneer dergelijke AI-systemen onvoldoende transparant, verklaarbaar en gedocumenteerd zijn. Het is daarom passend om een aantal AI-systemen dat bedoeld is voor gebruik in de context van rechtshandhaving, waar nauwkeurigheid, betrouwbaarheid en transparantie bijzonder belangrijk zijn om negatieve effecten te voorkomen, het vertrouwen van het publiek te behouden en de verantwoording en doeltreffende voorziening in rechte te waarborgen, als systemen met een hoog risico te classificeren, voor zover het gebruik daarvan is toegestaan op grond van het toepasselijke Unierecht en nationale recht.

Met het oog op de aard van de activiteiten en de hieraan gerelateerde risico's moeten deze AI-systemen met een hoog risico met name AI-systemen omvatten die bedoeld zijn om door of namens rechtshandhavingsinstanties of instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt voor het beoordelen van het risico dat een natuurlijk persoon potentieel slachtoffer van strafbare feiten wordt, zoals leugendetector tests en vergelijkbare instrumenten, voor het beoordelen van de betrouwbaarheid van bewijsmateriaal tijdens het onderzoek naar of de vervolging van strafbare feiten en, voor zover niet verboden op grond van deze verordening, voor het beoordelen van het risico dat een natuurlijk persoon een inbreuk pleegt of recidive pleegt, niet uitsluitend op basis van de profilering van natuurlijke personen of de beoordeling van persoonlijkheidskenmerken of het criminele gedrag van natuurlijke personen of groepen in het verleden, voor profilering in de loop van de opsporing, het onderzoek of de vervolging van strafbare feiten. AI-systemen die specifiek bedoeld zijn voor gebruik voor administratieve procedures van belasting- en douaneautoriteiten en door financiële-inlichtingeneenheden die administratieve taken uitvoeren en informatie analyseren overeenkomstig de antiwitwaswetgeving van de Unie, mogen niet worden geclassificeerd als AI-systemen met een hoog risico die worden gebruikt door rechtshandhavingsinstanties met het oog op het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten. Het gebruik van AI-instrumenten door rechtshandhavingsinstanties en andere relevante autoriteiten mag geen factor van ongelijkheid of uitsluiting worden. De gevolgen van het gebruik van AI-instrumenten voor de rechten van verdediging van verdachten mogen niet worden genegeerd, met name het probleem om betekenisvolle informatie over de werking van die systemen te verkrijgen, en het daaruit voortvloeiende probleem om de resultaten daarvan voor de rechtbank aan te vechten, met name door natuurlijke personen tegen wie een onderzoek loopt.

- (60) AI-systemen die worden gebruikt op het gebied van migratie, asiel en grenstoezichtsbeheer hebben gevolgen voor personen die vaak in een bijzonder kwetsbare positie verkeren en die afhankelijk zijn van de uitkomst van de acties van de bevoegde overheidsinstanties. De nauwkeurigheid, niet-discriminerende aard en transparantie van de AI-systemen die in deze context worden gebruikt, zijn derhalve van bijzonder belang om de eerbiediging van de grondrechten van de betrokken personen te waarborgen, en met name hun recht op vrij verkeer, non-discriminatie, bescherming van privéleven en persoonsgegevens, internationale bescherming en goed bestuur. Het is derhalve passend om AI-systemen, voor zover het gebruik daarvan is toegestaan op grond van het toepasselijke Unierecht en nationale recht, als systemen met een hoog risico te classificeren wanneer zij bedoeld zijn om te worden gebruikt door of namens de bevoegde overheidsinstanties of instellingen, organen of instanties van de Unie die taken op het gebied van migratie, asiel en grenstoezichtsbeheer uitvoeren, zoals leugendetectortests en vergelijkbare instrumenten, om bepaalde risico's te beoordelen die natuurlijke personen vormen die het grondgebied van een lidstaat binnenkomen of een visum- of asielaanvraag indienen, om bevoegde overheidsinstanties bij te staan bij de behandeling, met inbegrip van een gerelateerde beoordeling van de betrouwbaarheid van bewijsmateriaal, van aanvragen voor asiel, visa en verblijfsvergunningen en hieraan gerelateerde klachten teneinde vast te stellen of de natuurlijke personen die een status aanvragen, hiervoor in aanmerking komen, met het oog op het opsporen, het herkennen of identificeren van natuurlijke personen in het kader van migratie, asiel en grenstoezichtsbeheer, met uitzondering van de verificatie van reisdocumenten.

AI-systemen op het gebied van migratie, asiel en grenstoezichtsbeheer die onder deze verordening vallen, moeten in overeenstemming zijn met de desbetreffende procedurele eisen die zijn vastgelegd in Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad³², Richtlijn 2013/32/EU van het Europees Parlement en de Raad³³ en ander toepasselijk Unierecht. Het gebruik van AI-systemen in het kader van migratie, asiel en grenstoezichtsbeheer mag in geen geval door de lidstaten of de instellingen, organen of instanties van de Unie worden gebruikt als middel om hun internationale verplichtingen uit hoofde van het VN-Verdrag betreffende de status van vluchtelingen, ondertekend te Genève op 28 juli 1951 en gewijzigd bij het Protocol van 31 januari 1967, te omzeilen. Evenmin mogen zij worden gebruikt om op enigerlei wijze inbreuk te maken op het beginsel van non-refoulement of om veilige en doeltreffende legale wegen naar het grondgebied van de Unie te ontzeggen, met inbegrip van het recht op internationale bescherming.

³² Verordening (EG) nr. 810/2009 van het Europees Parlement en de Raad van 13 juli 2009 tot vaststelling van een gemeenschappelijke visumcode (Visumcode) (PB L 243 van 15.9.2009, blz. 1).

³³ Richtlijn 2013/32/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende gemeenschappelijke procedures voor de toekenning en intrekking van de internationale bescherming (PB L 180 van 29.6.2013, blz. 60).

- (61) Bepaalde AI-systemen die bedoeld zijn voor de rechtsbedeling en democratische processen moeten als systemen met een hoog risico worden geclassificeerd gezien hun mogelijk aanzienlijke effecten op de democratie, de rechtsstaat, de individuele vrijheden en het recht op een doeltreffende voorziening in rechte en op een onpartijdig gerecht. Om de risico's van potentiële vertekeningen, fouten en ondoorzichtigheid aan te pakken, is het met name passend om AI-systemen met een hoog risico die bedoeld zijn om door of namens een gerechtelijke instantie te worden gebruikt voor de ondersteuning van gerechtelijke autoriteiten bij het onderzoeken en uitleggen van feiten en het recht en bij het toepassen van het recht op een concrete reeks feiten, als systemen met een hoog risico aan te merken. AI-systemen die bedoeld zijn om door organen voor alternatieve geschillenbeslechting voor die doeleinden te worden gebruikt, moeten ook als systemen met een hoog risico worden beschouwd indien de resultaten van de alternatieve geschillenbeslechtingsprocedure rechtsgevolgen hebben voor de partijen. Het gebruik van AI-instrumenten kan de beslissingsbevoegdheid van rechters of de onafhankelijkheid van de rechterlijke macht ondersteunen, maar mag deze niet vervangen: de uiteindelijke besluitvorming moet een door de mens aangestuurde activiteit blijven. De classificatie van AI-systemen als AI-systemen met een hoog risico mag echter geen AI-systemen betreffen die bedoeld zijn voor louter ondersteunende administratieve activiteiten die geen gevolgen hebben voor de daadwerkelijke rechtsbedeling in afzonderlijke zaken, zoals de anonimisering of pseudonimisering van rechterlijke beslissingen, documenten of data, de communicatie tussen personeelsleden en administratieve taken.

- (62) Onverminderd de regels van Verordening (EU) 2024/... van het Europees Parlement en de Raad³⁴⁺, en om de risico's van ongepaste externe inmenging van buitenaf in het in artikel 39 van het Handvest verankerde stemrecht en van onevenredige gevolgen voor democratische processen, democratie en de rechtsstaat aan te pakken, moeten AI-systemen die bedoeld zijn om de uitslag van een verkiezing of referendum of het stemgedrag van natuurlijke personen wanneer zij hun stem uitbrengen bij verkiezingen of referenda te beïnvloeden, worden geclassificeerd als AI-systemen met een hoog risico, met uitzondering van AI-systemen waarvan de output niet rechtstreeks is gericht op natuurlijke personen, zoals instrumenten voor het organiseren, optimaliseren en structureren van politieke campagnes vanuit administratief en logistiek oogpunt.
- (63) Het feit dat een AI-systeem uit hoofde van deze verordening als een AI-systeem met een hoog risico is geclassificeerd, mag niet aldus worden uitgelegd dat het gebruik van het systeem rechtmatig is op grond van andere handelingen van het Unierecht of op grond van nationaal recht dat verenigbaar is met het Unierecht, zoals met betrekking tot de bescherming van de persoonsgegevens, het gebruik van leugendetectors en vergelijkbare instrumenten of andere systemen voor het bepalen van de gemoedstoestand van natuurlijke personen. Een dergelijk gebruik mag nog steeds uitsluitend plaatsvinden in overeenstemming met de toepasselijke eisen die voortvloeien uit het Handvest en de toepasselijke handelingen van secundair Unierecht en nationaal recht. Deze verordening mag niet aldus worden uitgelegd dat zij voorziet in de rechtsgrondslag voor de verwerking van persoonsgegevens, met inbegrip van bijzondere categorieën persoonsgegevens, waar van toepassing, tenzij in deze verordening uitdrukkelijk anders is bepaald.

³⁴ Verordening (EU) 2024/... van het Europees Parlement en de Raad betreffende transparantie en gerichte politieke reclame (PB L, ..., ELI: ...).

⁺ PB: gelieve in de tekst het nummer in te vullen van de verordening in PE 90/23 (2021/0381(COD)) en de voetnoot te vervolledigen.

- (64) Om de risico's van AI-systemen met een hoog risico die in de handel zijn gebracht of in gebruik zijn gesteld te beperken en om te zorgen voor een hoog niveau van betrouwbaarheid, moeten op AI-systemen met een hoog risico bepaalde dwingende eisen van toepassing zijn, rekening houdend met het beoogde doel en de context van het gebruik van het AI-systeem en in overeenstemming met het systeem voor risicobeheer dat door de aanbieder wordt vastgesteld. De maatregelen die de aanbieders met het oog op het voldoen aan de dwingende eisen van deze verordening hebben vastgesteld, moeten rekening gehouden met de algemeen erkende stand van de techniek op het gebied van AI, evenredig en doeltreffend zijn teneinde de doelstellingen van deze verordening te verwezenlijken. Op basis van het nieuwe wetgevingskader, zoals uiteengezet in de mededeling van de Commissie “De “Blauwe Gids” voor de uitvoering van de productvoorschriften van de EU 2022”, is de algemene regel dat meer dan een rechtshandeling van de harmonisatiewetgeving van de Unie van toepassing kan zijn op één product, aangezien een product alleen mag worden aangeboden of in gebruik worden gesteld wanneer het voldoet aan alle toepasselijke harmonisatiewetgeving van de Unie. De gevaren van AI-systemen die onder de eisen van deze verordening vallen, hebben betrekking op andere aspecten dan de bestaande harmonisatiewetgeving van de Unie en daarom zouden de eisen van deze verordening een aanvulling vormen op het bestaande corpus van de harmonisatiewetgeving van de Unie. Machines of medische hulpmiddelen die een AI-systeem bevatten, kunnen bijvoorbeeld risico's inhouden die niet worden gedekt door de essentiële gezondheids- en veiligheidseisen van de toepasselijke geharmoniseerde wetgeving van de Unie, aangezien die sectorale wetgeving geen betrekking heeft op risico's die specifiek zijn voor AI-systemen.

Dit vereist een gezamenlijke en aanvullende toepassing van de verschillende wetgeving. Om consistentie te waarborgen en onnodige administratieve lasten en onnodige kosten te vermijden, moeten aanbieders van een product dat een of meer AI-systemen met een hoog risico bevat waarop de eisen van deze verordening en van de in een bijlage bij deze verordening vermelde harmonisatiewetgeving van de Unie op basis van het nieuwe wetgevingskader van toepassing zijn, flexibel zijn met betrekking tot operationele beslissingen over de wijze waarop ervoor kan worden gezorgd dat een product dat een of meer AI-systemen bevat, op optimale wijze voldoet aan alle toepasselijke eisen van die geharmoniseerde wetgeving van de Unie. Die flexibiliteit kan bijvoorbeeld inhouden dat de aanbieder besluit om een deel van de nodige test- en rapportageprocessen en de krachtens deze verordening te verstrekken informatie en documentatie op te nemen in de reeds bestaande documentatie en procedures die vereist zijn uit hoofde van bestaande harmonisatiewetgeving van de Unie die is gebaseerd is op het nieuwe wetgevingskader en in een bijlage bij deze verordening wordt vermeld. Dit mag op geen enkele wijze afbreuk doen aan de verplichting van de aanbieder om aan alle toepasselijke eisen te voldoen.

- (65) Het systeem voor risicobeheer moet bestaan uit een tijdens de gehele levensduur van een AI-systeem met een hoog risico doorlopend en gepland iteratief proces. Dit proces moet gericht zijn op het vaststellen en beperken van de relevante risico's van AI-systemen voor de gezondheid, de veiligheid en de grondrechten. Het systeem voor risicobeheer moet periodiek worden geëvalueerd en geactualiseerd om de blijvende doeltreffendheid ervan te waarborgen, alsook de motivering en de documentatie van eventuele significante besluiten en maatregelen die op grond van deze verordening zijn genomen. Dit proces moet ervoor zorgen dat de aanbieder de risico's of negatieve effecten vaststelt en risicobeperkende maatregelen uitvoert voor de bekende en de redelijkerwijs te voorziene risico's van AI-systemen voor de gezondheid, veiligheid en grondrechten in het licht van het beoogde doel ervan en redelijkerwijs te voorzien misbruik, met inbegrip van de mogelijke risico's die voortvloeien uit de wisselwerking tussen het AI-systeem en de omgeving waarin het werkt. Het systeem voor risicobeheer moet de passendste risicobeheersmaatregelen vaststellen in het licht van de stand van de techniek op het gebied van AI. Bij het vaststellen van de passendste risicobeheersmaatregelen moet de aanbieder de gemaakte keuzes documenteren en toelichten en, in voorkomend geval, deskundigen en externe belanghebbenden erbij betrekken. Bij het vaststellen van het redelijkerwijs te voorzien misbruik van AI-systemen met een hoog risico moet de aanbieder aandacht hebben voor het gebruik van AI-systemen waarvan, hoewel zij niet rechtstreeks onder het beoogde doel vallen en niet in de gebruiksinstructies worden vermeld, redelijkerwijs mag worden verwacht dat zij kunnen voortvloeien uit gemakkelijk voorspelbaar menselijk gedrag in de context van de specifieke kenmerken en het gebruik van een bepaald AI-systeem. Eventuele bekende of te voorziene omstandigheden in verband met het gebruik van het AI-systeem met een hoog risico in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik die kunnen leiden tot risico's voor de gezondheid en veiligheid of de grondrechten, moeten worden opgenomen in de gebruiksinstructies die de aanbieder ter beschikking heeft gesteld. Dit moet ervoor zorgen dat de gebruiksverantwoordelijke hiervan op de hoogte is en hiermee rekening houdt bij het gebruik van het AI-systeem met een hoog risico. Het vaststellen en uitvoeren van risicobeperkende maatregelen voor te voorzien misbruik uit hoofde van deze verordening mag van de aanbieder geen voor het AI-systeem met een hoog risico specifieke aanvullende training vergen om te voorzien misbruik aan te pakken. De aanbieders worden echter aangemoedigd dergelijke aanvullende trainingsmaatregelen te overwegen om redelijkerwijs te voorzien misbruik waar nodig en passend te beperken.

- (66) Op AI-systemen met een hoog risico moeten eisen van toepassing zijn met betrekking tot risicobeheer, de kwaliteit en relevantie van de gebruikte datasets, technische documentatie en registratie, transparantie en het verstrekken van informatie aan gebruiksverantwoordelijken, menselijk toezicht en robuustheid, nauwkeurigheid en cyberbeveiliging. Deze eisen zijn noodzakelijk om de risico's voor de gezondheid, veiligheid en grondrechten te verminderen. Aangezien er geen andere maatregelen die de handel in mindere mate beperken, redelijkerwijs beschikbaar zijn, vormen die eisen geen ongerechtvaardigde beperkingen van de handel.

(67) Kwalitatief hoogwaardige data en de toegang hiertoe is van wezenlijk belang voor het bieden van structuur en het waarborgen van de prestaties van veel AI-systemen, met name wanneer technieken worden gebruikt waarbij modellen worden getraind, om ervoor te zorgen dat AI-systemen met een hoog risico zoals beoogd en veilig werken en geen bron van discriminatie worden die uit hoofde van het Unierecht verboden is. Kwalitatief hoogwaardige datasets voor training, validatie en tests vereisen de uitvoering van passende praktijken voor datagovernance en -beheer. Datasets voor training, validatie en tests, met inbegrip van het labelen ervan, moeten relevant, voldoende representatief, en zoveel mogelijk foutenvrij en volledig met het oog op het beoogde doel van het systeem zijn. Om de naleving van het Unierecht inzake gegevensbescherming, zoals Verordening (EU) 2016/679, te vergemakkelijken, moeten praktijken voor datagovernance en beheer, in het geval van persoonsgegevens, transparantie met betrekking tot het oorspronkelijke doel van de dataverzameling omvatten. De datasets moeten bovendien de passende statistische kenmerken hebben, waaronder met betrekking tot de personen of groepen personen in verband met wie de AI-systemen met een hoog risico moeten worden gebruikt, met bijzondere aandacht voor het tegengaan van mogelijke vertekeningen in de datasets, die waarschijnlijk gevolgen hebben voor de gezondheid en de veiligheid van personen, nadelige effecten hebben op de grondrechten, of leiden tot discriminatie die op grond van het Unierecht verboden is, vooral wanneer data-outputs invloed hebben op inputs voor toekomstige operaties (“feedback loops”). Vertekeningen kunnen bijvoorbeeld inherent zijn aan de onderliggende datasets, met name wanneer historische gegevens worden gebruikt of gegenereerd wanneer de systemen onder reële omstandigheden worden toegepast.

De resultaten die door AI-systemen worden aangeboden, kunnen worden beïnvloed door dergelijke inherente vertekeningen, die vaak geleidelijk groter worden en daarmee bestaande discriminatie bestendigen en verergeren, met name voor personen die tot bepaalde kwetsbare groepen behoren, waaronder raciale of etnische groepen. De eis dat de datasets zoveel mogelijk volledig en foutenvrij moeten zijn, mag geen invloed hebben op het gebruik van privacybeschermende technieken in het kader van de ontwikkeling en het testen van AI-systemen. Ten aanzien van datasets moet, voor zover vereist gezien het beoogde doel hiervan, met name rekening worden gehouden met de kenmerken, eigenschappen of elementen die specifiek zijn voor een bepaalde geografische, contextuele, gedragsgerelateerde of functionele omgeving waarin het AI-systeem moet worden gebruikt. Aan de eisen inzake databeheer kan worden voldaan door een beroep te doen op derden die gecertificeerde nalevingsdiensten aanbieden, waaronder verificatie van datagovernance, integriteit van datasets, en datatraining, -validatie en -tests, voor zover de naleving van de datavereisten van deze verordening wordt gewaarborgd.

- (68) Voor de ontwikkeling en beoordeling van AI-systemen met een hoog risico moeten bepaalde actoren, zoals aanbieders, aangemelde instanties en andere relevante entiteiten, zoals Europese digitale-innovatiehubs, test- en experimenteerfaciliteiten en onderzoekers, toegang hebben tot kwalitatief hoogwaardige datasets op de gebieden waarop deze actoren activiteiten verrichten die verband houden met deze verordening en hiervan gebruik kunnen maken. Door de Commissie vastgestelde gemeenschappelijke Europese gegevensruimten en de vergemakkelijking van de gegevensuitwisseling tussen ondernemingen en de overheid in het algemeen belang zullen erg belangrijk zijn voor een betrouwbare, toerekenbare en niet-discriminerende toegang tot kwalitatief hoogwaardige data voor het trainen, valideren en testen van AI-systemen. Op het gebied van gezondheid zal de Europese ruimte voor gezondheidsgegevens bijvoorbeeld de niet-discriminerende toegang tot gezondheidsgegevens en de training van AI-algoritmen aan de hand van deze datasets vergemakkelijken op een wijze die de privacy waarborgt en die veilig, tijdig, transparant en betrouwbaar is, met een passend institutioneel beheer. Relevante bevoegde autoriteiten, waaronder sectorale autoriteiten, die de toegang tot data verlenen of ondersteunen, kunnen ook steun verlenen voor het verstrekken van kwalitatief hoogwaardige data voor het trainen, valideren en testen van AI-systemen.
- (69) Het recht op privacy en bescherming van persoonsgegevens moet gedurende de hele levenscyclus van het AI-systeem worden gewaarborgd. In dit verband zijn bij de verwerking van persoonsgegevens de beginselen van minimale gegevensverwerking en van gegevensbescherming door ontwerp en door standaardinstellingen, zoals vastgelegd in het Unierecht inzake gegevensbescherming, van toepassing. De maatregelen die aanbieders nemen om te zorgen voor de naleving van die beginselen, moeten niet alleen anonimisering en versleuteling omvatten, maar ook het gebruik van technologie die de toepassing van algoritmen op gegevens en de training van AI-systemen mogelijk maakt zonder de uitwisseling van de ruwe of gestructureerde gegevens zelf tussen partijen of het kopiëren daarvan, onverminderd de eisen inzake datagovernance waarin deze verordening voorziet.

- (70) Om het recht van anderen te beschermen tegen discriminatie die kan voortvloeien uit de vooringenomenheid (bias) in AI-systemen, moeten aanbieders, bij wijze van uitzondering, voor zover dit strikt noodzakelijk is om de opsporing en correctie van vertekeningen te waarborgen in verband met de AI-systemen met een hoog risico, mits passende waarborgen worden geboden voor de grondrechten en fundamentele vrijheden van natuurlijke personen en na toepassing van alle toepasselijke voorwaarden die in deze verordening, alsmede in de Verordeningen (EU) 2016/679 en (EU) 2018/1725 en Richtlijn (EU) 2016/680 zijn vastgelegd, ook bijzondere categorieën persoonsgegevens kunnen verwerken wanneer sprake is van een zwaarwegend algemeen belang in de zin van artikel 9, lid 2, punt g), van Verordening (EU) 2016/679 en artikel 10, lid 2, punt g), van Verordening (EU) 2018/1725.
- (71) Begrijpelijke informatie over de manier waarop AI-systemen met een hoog risico zijn ontwikkeld en hoe zij gedurende hun levensduur presteren, is essentieel om de traceerbaarheid van die systemen mogelijk te maken, om de overeenstemming met de eisen van deze verordening te controleren, en om de monitoring van de werking en de monitoring na het in handel brengen mogelijk te maken. Dit vereist de registratie en de beschikbaarheid van technische documentatie die de noodzakelijke data bevat om de overeenstemming van het AI-systeem met de desbetreffende eisen te beoordelen en de monitoring na het in handel brengen te vergemakkelijken. Dergelijke informatie moet de algemene kenmerken, mogelijkheden en beperkingen van het systeem omvatten, evenals algoritmen, data en gebruikte processen voor het trainen, testen en valideren, alsook documentatie met betrekking tot het desbetreffende systeem voor risicobeheer, en moet op heldere en begrijpelijke wijze zijn gesteld. De technische documentatie moet gedurende de levensduur van het AI-systeem op gepaste wijze actueel worden gehouden. Voorts moeten AI-systemen met een hoog risico dusdanig technisch zijn vormgegeven dat gebeurtenissen gedurende de levensduur van het systeem, automatisch worden geregistreerd door middel van “logs”.

- (72) Om problemen in verband met de ondoorzichtigheid en complexiteit van bepaalde AI-systemen aan te pakken en gebruiksverantwoordelijken te helpen hun verplichtingen uit hoofde van deze verordening na te komen, moet transparantie vereist zijn voor AI-systemen met een hoog risico voordat zij in de handel worden gebracht of in gebruik worden gesteld. AI-systemen met een hoog risico moeten zodanig zijn ontworpen dat gebruiksverantwoordelijken kunnen begrijpen hoe het AI-systeem werkt, de werking ervan kunnen evalueren en de sterke punten en beperkingen ervan kunnen begrijpen. AI-systemen met een hoog risico moeten vergezeld gaan van relevante documentatie in de vorm van gebruiksaanwijzingen. Deze informatie moet de kenmerken, mogelijkheden en beperkingen van de prestaties van het AI-systeem bevatten. Die elementen zouden informatie omvatten over mogelijke bekende en te voorziene omstandigheden in verband met het gebruik van het AI-systeem met een hoog risico, waaronder handelingen van de gebruiksverantwoordelijke die van invloed kunnen zijn op het gedrag en de prestaties van het systeem, op grond waarvan het AI-systeem risico's kan veroorzaken voor de gezondheid, veiligheid en grondrechten, over de wijzigingen die vooraf zijn bepaald en beoordeeld met het oog op conformiteit door de aanbieder, en over de relevante maatregelen voor menselijk toezicht, waaronder de maatregelen om de interpretatie van de output van het AI-systeem door de gebruiksverantwoordelijken te vergemakkelijken. Transparantie, met inbegrip van de bijbehorende gebruiksaanwijzingen, moet gebruiksverantwoordelijken helpen bij het gebruik van het systeem, en hen helpen onderbouwde beslissingen te nemen. De gebruiksverantwoordelijken moeten onder meer beter in staat zijn om het juiste systeem te kiezen dat zij voornemens zijn te gebruiken in het licht van de verplichtingen die op hen van toepassing zijn, om te worden geïnformeerd over het beoogde en uitgesloten gebruik, en om het AI-systeem correct en op passende wijze te gebruiken. Om de leesbaarheid en toegankelijkheid van de informatie in de gebruiksaanwijzingen te verbeteren, moeten, waar passend, illustratieve voorbeelden worden opgenomen, bijvoorbeeld over de beperkingen en het beoogde en uitgesloten gebruik van het AI-systeem. De aanbieders moeten ervoor zorgen dat alle documentatie, met inbegrip van de gebruiksaanwijzingen, zinvolle, volledige, toegankelijke en begrijpelijke informatie bevat, die rekening houdt met de behoeften en de te verwachten kennis van de beoogde gebruiksverantwoordelijken. De gebruiksaanwijzingen moeten beschikbaar worden gesteld in een taal die de beoogde gebruiksverantwoordelijken gemakkelijk kunnen begrijpen, welke de betrokken lidstaat bepaalt.

- (73) AI-systemen met een hoog risico moeten op zodanige wijze worden ontworpen en ontwikkeld dat natuurlijke personen toezicht kunnen houden op de werking ervan en dat zij zoals beoogd worden gebruikt, en dat de gevolgen ervan gedurende de levenscyclus van het systeem worden aangepakt. Daartoe moeten passende maatregelen voor menselijk toezicht worden bepaald door de aanbieder van het systeem voordat het in de handel wordt gebracht of in gebruik wordt gesteld. Dergelijke maatregelen moeten, waar passend, met name waarborgen dat voor het systeem ingebouwde operationele beperkingen gelden die niet door het systeem zelf kunnen worden omzeild, dat het systeem reageert op de menselijke operator en dat de natuurlijke personen aan wie de taak van het menselijk toezicht is toegewezen, beschikken over de noodzakelijke competenties, opleiding en autoriteit om deze taak uit te voeren. Het is in voorkomend geval ook van essentieel belang dat AI-systemen met een hoog risico mechanismen bevatten om een natuurlijke persoon aan wie de taak van het menselijk toezicht is toegewezen, te begeleiden en te informeren zodat deze persoon geïnformeerd kan beslissen of, wanneer en hoe moet worden ingegrepen om negatieve gevolgen of risico's te voorkomen, of om het systeem stop te zetten als het niet naar behoren functioneert. Gezien de aanzienlijke gevolgen voor personen in geval van een onjuiste match door bepaalde systemen voor biometrische identificatie, is het passend te voorzien in een voorschrift voor verscherpt menselijk toezicht voor die systemen, zodat er door de gebruiksverantwoordelijke geen maatregelen of beslissingen kunnen worden genomen op basis van de identificatie door het systeem, tenzij deze identificatie door ten minste twee natuurlijke personen afzonderlijk is geverifieerd en bevestigd. Deze personen kunnen afkomstig zijn van een of meer entiteiten en deze functie kan worden vervuld door de persoon die het systeem exploiteert of gebruikt. Deze eis mag geen onnodige lasten of vertragingen met zich meebrengen en het kan volstaan dat de afzonderlijke verificaties door de verschillende personen automatisch worden geregistreerd in de logbestanden die door het systeem worden gegenereerd. Gezien de specifieke kenmerken van rechtshandhaving, migratie, grenstoezicht en asiel, mag deze eis niet van toepassing zijn wanneer het Unierecht of het nationale recht de toepassing van dat vereiste onevenredig acht.

- (74) AI-systemen met een hoog risico moeten gedurende hun levenscyclus consistent presteren en een passend niveau van nauwkeurigheid, robuustheid en cyberbeveiliging behalen in het licht van het beoogde doel ervan en overeenstemming met de algemeen erkende stand van de techniek. De Commissie en relevante organisaties en belanghebbenden worden aangemoedigd om terdege rekening te houden met de beperking van risico's en de negatieve gevolgen van het AI-systeem. Het verwachte prestatieniveau moet in de bijbehorende gebruiksaanwijzingen worden vermeld. Aanbieders wordt verzocht die informatie aan de gebruiksverantwoordelijken mee te delen op een manier die duidelijk en gemakkelijk te begrijpen is en die geen misleidende opmerkingen bevat of ruimte biedt voor misverstanden. Het Unierecht inzake wettelijke metrologie, waaronder de Richtlijnen 2014/31/EU³⁵ en 2014/32/EU³⁶ van het Europees Parlement en de Raad, heeft tot doel de nauwkeurigheid van metingen te waarborgen en de transparantie en eerlijkheid van handelstransacties te bevorderen. In dat verband moet de Commissie, in samenwerking met relevante belanghebbenden en organisaties, zoals metrologie- en benchmarkingautoriteiten, waar passend, de ontwikkeling van benchmarks en meetmethoden voor AI-systemen aanmoedigen. Daarbij moet de Commissie nota nemen en samenwerken met internationale partners die werken rond metrologie en relevante meetindicatoren met betrekking tot AI.

³⁵ Richtlijn 2014/31/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van niet-automatische weegwerktuigen (PB L 96 van 29.3.2014, blz. 107).

³⁶ Richtlijn 2014/32/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van meetinstrumenten (PB L 96 van 29.3.2014, blz. 149).

- (75) Technische robuustheid is een essentiële eis voor AI-systemen met een hoog risico. Deze systemen moeten bestand zijn tegen schadelijk of anderszins ongewenst gedrag dat kan voortvloeien uit de beperkingen binnen de systemen of de omgeving waarin de systemen opereren (bv. fouten, onregelmatigheden, onverwachte situaties). Daarom moeten technische en organisatorische maatregelen worden getroffen om de robuustheid van AI-systemen met een hoog risico te waarborgen, bijvoorbeeld door passende technische oplossingen te ontwerpen en te ontwikkelen om schadelijk of anderszins ongewenst gedrag te voorkomen of tot een minimum te beperken. Deze technische oplossing kan bijvoorbeeld bestaan uit mechanismen die het systeem in staat stellen zijn werking veilig te onderbreken (storingsbeveiligingsplannen) wanneer zich bepaalde anomalieën voordoen of wanneer de werking buiten bepaalde vooraf bepaalde grenzen plaatsvindt. Wanneer niet tegen deze risico's wordt beschermd, kan dit leiden tot veiligheidseffecten of negatieve gevolgen voor de grondrechten, bijvoorbeeld als gevolg van foutieve beslissingen of een onjuiste of vertekende output die door het AI-systeem wordt gegenereerd.
- (76) Cyberbeveiliging is cruciaal om te waarborgen dat AI-systemen bestand zijn tegen pogingen van kwaadwillige derden die gebruikmaken van de kwetsbaarheden van het systeem om het gebruik, het gedrag of de prestaties ervan te wijzigen of de veiligheidskenmerken ervan in gevaar te brengen. Bij cyberaanvallen tegen AI-systemen kunnen AI-specifieke activa worden gebruikt, zoals trainingsdatasets (bv. datavervuiling) of getrainde modellen (bv. vijandige aanvallen of membership inference), of kwetsbaarheden in de digitale activa van het AI-systeem of de onderliggende ICT-infrastructuur worden benut. Om te zorgen voor een niveau van cyberbeveiliging dat aansluit op de risico's, moeten aanbieders van AI-systemen met een hoog risico derhalve passende maatregelen zoals veiligheidscontroles nemen, waarbij ook op passende wijze rekening wordt gehouden met de onderliggende ICT-infrastructuur.

(77) Onverminderd de bij deze verordening vastgestelde eisen met betrekking tot robuustheid en nauwkeurigheid kunnen AI-systemen met een hoog risico die onder het toepassingsgebied van een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen vallen, overeenkomstig die verordening de naleving van de cyberbeveiligingseisen van onderhavige verordening aantonen door te voldoen aan de essentiële cyberbeveiligingseisen van die verordening. Wanneer AI-systemen met een hoog risico voldoen aan de essentiële eisen van een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen, moeten zij worden geacht in overeenstemming te zijn met de cyberbeveiligingseisen van deze verordening, voor zover de naleving van die eisen wordt aangetoond in de EU-conformiteitsverklaring of delen daarvan die is afgegeven op grond van die verordening. Daartoe moet bij de beoordeling van de cyberbeveiligingsrisico's die verbonden zijn aan een product met digitale elementen dat overeenkomstig deze verordening als AI-systeem met een hoog risico is geclassificeerd, welke wordt uitgevoerd uit hoofde van een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen, rekening worden gehouden met risico's voor de cyberweerbaarheid van een AI-systeem tegen pogingen van ongeautoriseerde derden om het gebruik, het gedrag of de prestaties ervan te wijzigen, en met AI-specifieke kwetsbaarheden zoals datavervuiling of vijandige aanvallen, alsook, voor zover relevant, risico's voor de grondrechten zoals op grond van deze verordening is vereist.

(78) De conformiteitsbeoordelingsprocedure waarin deze verordening voorziet, moet van toepassing zijn op de essentiële cyberbeveiligingseisen van een product met digitale elementen dat onder een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen valt en op grond van deze verordening als AI-systeem met een hoog risico is geclassificeerd. Deze regel mag echter niet leiden tot een verlaging van het vereiste betrouwbaarheidsniveau voor kritieke producten met digitale elementen die onder een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen vallen. In afwijking van deze regel zijn AI-systemen met een hoog risico die onder het toepassingsgebied van deze verordening vallen en eveneens op grond van een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen als belangrijke en kritieke producten met digitale elementen zijn geclassificeerd en waarop de in een bijlage bij deze verordening vastgelegde conformiteitsbeoordelingsprocedure op basis van interne controle van toepassing is, derhalve onderworpen aan de conformiteitsbeoordelingsbepalingen van een verordening van het Europees Parlement en de Raad betreffende horizontale cyber-beveiligings-vereisten voor producten met digitale elementen voor zover het de essentiële cyberbeveiligingseisen van die verordening betreft. In dat geval moeten de in een bijlage bij deze verordening vastgelegde respectieve bepalingen inzake conformiteitsbeoordeling op basis van interne controle van toepassing zijn op alle andere aspecten die onder die verordening vallen. Voortbouwend op de kennis en deskundigheid van Enisa inzake het cyberbeveiligingsbeleid en de taken die krachtens Verordening (EU) 2019/881 van het Europees Parlement en de Raad³⁷ aan Enisa zijn toegewezen, moet de Commissie op het gebied van kwesties in verband met de cyberbeveiliging van AI-systemen samenwerken met Enisa.

³⁷ Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

- (79) Het is passend dat een specifieke natuurlijke of rechtspersoon, die als aanbieder wordt aangemerkt, de verantwoordelijkheid neemt voor het in de handel brengen of in gebruik stellen van een AI-systeem met een hoog risico, ongeacht of deze natuurlijke of rechtspersoon de persoon is die het systeem heeft ontworpen of ontwikkeld.
- (80) Als ondertekenaars van het Verdrag van de Verenigde Naties inzake de rechten van personen met een handicap zijn de Unie en de lidstaten wettelijk verplicht personen met een handicap te beschermen tegen discriminatie en hun gelijkheid te bevorderen, ervoor te zorgen dat personen met een handicap op voet van gelijkheid met anderen toegang hebben tot informatie- en communicatietechnologieën en -systemen, en de eerbiediging van de privacy van personen met een handicap te waarborgen. Gezien het toenemende belang en gebruik van AI-systemen moet de toepassing van universele ontwerpbeginnselen op alle nieuwe technologieën en diensten zorgen voor volledige en gelijke toegang voor iedereen die mogelijk gevolgen ondervindt van of gebruikmaakt van AI-technologieën, met inbegrip van personen met een handicap, op een manier waarbij ten volle rekening wordt gehouden met hun inherente waardigheid en diversiteit. Het is daarom van essentieel belang dat aanbieders ervoor zorgen dat zij voldoen aan de toegankelijkheidseisen, alsook aan de Richtlijnen (EU) 2016/2102 van het Europees Parlement en de Raad³⁸ en (EU) 2019/882. Aanbieders moeten ervoor zorgen dat door ontwerp aan deze eisen wordt voldaan. De nodige maatregelen moeten daarom zo goed mogelijk in het ontwerp van AI-systemen met een hoog risico worden geïntegreerd.

³⁸ Richtlijn (EU) 2016/2102 van het Europees Parlement en de Raad van 26 oktober 2016 inzake de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties (PB L 327 van 2.12.2016, blz. 1).

- (81) De aanbieder moet een gedegen systeem voor kwaliteitsbeheer vaststellen, zorgen voor het doorlopen van de vereiste conformiteitsbeoordelingsprocedure, de relevante documentatie opstellen en een robuust systeem vaststellen voor monitoring na het in de handel brengen. Aanbieders van AI-systemen met een hoog risico die onderworpen zijn aan verplichtingen met betrekking tot kwaliteitsbeheersystemen uit hoofde van het desbetreffende sectorale Unierecht, moeten de mogelijkheid hebben om de elementen van het kwaliteitsbeheersysteem waarin deze verordening voorziet, op te nemen als onderdeel van het bestaande kwaliteitsbeheersysteem waarin dat andere sectorale Unierecht voorziet. Bij toekomstige normalisatieactiviteiten of in richtsnoeren van de Commissie moet ook rekening worden gehouden met de complementariteit tussen deze verordening en het bestaande sectorale Unierecht. Overheidsinstanties die AI-systemen met een hoog risico in gebruik stellen voor eigen gebruik mogen de regels voor het systeem voor kwaliteitsbeheer goedkeuren en uitvoeren als onderdeel van het systeem voor kwaliteitsbeheer dat, naargelang het geval, op nationaal of regionaal niveau is goedgekeurd, rekening houdend met de specifieke kenmerken van de sector en de competenties en organisatie van de overheidsinstantie in kwestie.

- (82) Om de handhaving van deze verordening mogelijk te maken en te zorgen voor een gelijk speelveld voor operatoren en rekening houdend met de verschillende vormen waarin digitale producten beschikbaar kunnen worden gesteld, is het van belang dat onder alle omstandigheden wordt gewaarborgd dat een persoon die in de Unie is gevestigd de autoriteiten alle noodzakelijke informatie kan verstrekken over de conformiteit van een AI-systeem. Voordat zij hun AI-systemen beschikbaar stellen in de Unie, moeten aanbieders die in derde landen zijn gevestigd derhalve per schriftelijke machtiging een gemachtigde aanwijzen die is gevestigd in de Unie. Deze gemachtigde vervult een spilfunctie bij de waarborging van de conformiteit van de door niet in de Unie gevestigde aanbieders in de handel gebrachte of in gebruik gestelde AI-systemen met een hoog risico en in zijn hoedanigheid van hun in de Unie gevestigde contactpersoon.
- (83) Gezien de aard en complexiteit van de waardeketen voor AI-systemen en in lijn met het nieuwe wetgevingskader is het van essentieel belang rechtszekerheid te waarborgen en de naleving van deze verordening te vergemakkelijken. Daarom is het van belang de rol en de specifieke verplichtingen van betrokken operatoren in die hele waardeketen, zoals importeurs en distributeurs die kunnen bijdragen tot de ontwikkeling van AI-systemen, te verduidelijken. In bepaalde situaties kunnen deze operatoren in meer dan één rol tegelijkertijd optreden en moeten zij derhalve alle relevante verplichtingen die aan die rollen zijn verbonden, samen vervullen. Een operator kan bijvoorbeeld tegelijkertijd als distributeur en als importeur optreden.

- (84) Om rechtszekerheid te waarborgen, moet worden verduidelijkt dat, onder bepaalde specifieke voorwaarden, om het even welke distributeur, importeur, gebruiksverantwoordelijke of andere derde moet worden beschouwd als aanbieder van een AI-systeem met een hoog risico en deze derhalve alle relevante verplichtingen moet nakomen. Dit zou het geval zijn als die partij haar naam of merk op een reeds in de handel gebracht of in gebruik gesteld AI-systeem met een hoog risico zet, onverminderd contractuele regelingen waarin wordt bepaald dat de verplichtingen anders worden toegewezen. Dit zou ook het geval zijn als die partij een substantiële wijziging aanbrengt aan een reeds in de handel gebracht of in gebruik gesteld AI-systeem met een hoog risico en dit op zodanige wijze doet dat het een AI-systeem met een hoog risico overeenkomstig deze verordening blijft, of als zij het beoogde doel van een AI-systeem, met inbegrip van een AI-systeem voor algemene doeleinden, dat niet als een AI-systeem met een hoog risico is geclassificeerd en reeds in de handel is gebracht of in gebruik is gesteld, op zodanige wijze wijzigt dat het AI-systeem een AI-systeem met een hoog risico overeenkomstig deze verordening wordt. Die bepalingen moeten van toepassing zijn onverminderd specifiekere bepalingen in bepaalde harmonisatiewetgeving van de Unie op basis van het nieuwe wetgevingskader waarmee deze verordening gezamenlijk moet worden toegepast. Zo moet artikel 16, lid 2, van Verordening (EU) 2017/745, waarin is bepaald dat bepaalde wijzigingen niet mogen worden beschouwd als een wijziging van een hulpmiddel die gevolgen kan hebben voor de naleving van de toepasselijke eisen, van toepassing blijven op AI-systemen met een hoog risico die medische hulpmiddelen zijn in de zin van die verordening.

- (85) AI-systemen voor algemene doeleinden kunnen worden gebruikt als standalone AI-systeem met een hoog risico of als component van AI-systemen met een hoog risico. Daarom moeten de aanbieders van deze systemen vanwege de specifieke aard ervan en om een eerlijke verdeling van verantwoordelijkheden in de AI-waardeketen te waarborgen, ongeacht of zij als AI-systemen met een hoog risico als zodanig door andere aanbieders of als componenten van AI-systemen met een hoog risico kunnen worden gebruikt en tenzij in deze verordening anders is bepaald, nauw samenwerken met de aanbieders van de betrokken AI-systemen met een hoog risico, om hun naleving van de verplichtingen uit hoofde van deze verordening mogelijk te maken, en met de bevoegde autoriteiten zoals vastgelegd in deze verordening.
- (86) Wanneer, onder de in deze verordening vastgelegde voorwaarden, de aanbieder die het AI-systeem oorspronkelijk in de handel heeft gebracht of in gebruik heeft gesteld, voor de toepassing van deze verordening niet langer als de aanbieder mag worden beschouwd, en indien die aanbieder de wijziging van het AI-systeem in een AI-systeem met een hoog risico niet uitdrukkelijk heeft uitgesloten, moet de eerstgenoemde aanbieder niettemin nauw samenwerken en de nodige informatie beschikbaar stellen, en de redelijkerwijs te verwachten technische toegang en andere bijstand verstrekken die nodig is voor de naleving van de bij deze verordening vastgestelde verplichtingen, met name wat betreft de naleving van de conformiteitsbeoordeling van AI-systemen met een hoog risico.
- (87) Wanneer een AI-systeem met een hoog risico dat een veiligheidscomponent is van een product dat valt onder het toepassingsgebied van de harmonisatiewetgeving van de Unie op basis van het nieuwe wetgevingskader, niet onafhankelijk van het product in de handel wordt gebracht of in gebruik wordt gesteld, moet de productfabrikant, zoals gedefinieerd in die wetgeving, voorts de verplichtingen van de aanbieder naleven, zoals vastgelegd in deze verordening, en moet hij er met name voor zorgen dat het AI-systeem dat is opgenomen in het eindproduct in overeenstemming is met de eisen van deze verordening.

- (88) In de hele de AI-waardeketen worden vaak door meerdere partijen AI-systemen, instrumenten en diensten geleverd, alsook onderdelen of processen, die door de aanbieder in het AI-systeem worden geïntegreerd, een en ander met verscheidene doelstellingen, waaronder het (opnieuw) trainen, testen en evalueren van modellen, de integratie in software, of andere aspecten van modelontwikkeling. Die partijen hebben een belangrijke rol te spelen in de waardeketen ten aanzien van de aanbieder van het AI-systeem met een hoog risico waarin hun AI-systemen, instrumenten, diensten, componenten of processen zijn geïntegreerd, en moeten deze aanbieder bij schriftelijke overeenkomst de nodige informatie, capaciteiten, technische toegang en andere bijstand verstrekken op basis van de algemeen erkende stand van de techniek, teneinde de aanbieder in staat te stellen volledig te voldoen aan de verplichtingen van deze verordening, zonder afbreuk te doen aan hun eigen intellectuele-eigendomsrechten of bedrijfsgeheimen.
- (89) Derden die andere instrumenten, diensten, processen of AI-componenten dan AI-modellen voor algemene doeleinden toegankelijk maken voor het publiek, mogen niet worden verplicht te voldoen aan eisen die gericht zijn op de verantwoordelijkheden in de AI-waardeketen, met name ten aanzien van de aanbieder die deze heeft gebruikt of geïntegreerd, wanneer die instrumenten, diensten, processen of AI-componenten onder een vrije en opensource licentie toegankelijk worden gemaakt. Ontwikkelaars van vrije en opensource-AI-componenten, diensten, processen of andere AI-componenten dan AI-modellen voor algemene doeleinden moeten echter worden aangemoedigd om algemeen aanvaarde documentatiepraktijken, zoals model- en gegevenskaarten, toe te passen als een manier om de uitwisseling van informatie in de hele AI-waardeketen te versnellen, in het kader van de bevordering van betrouwbare AI-systemen in de Unie.

- (90) De Commissie kan vrijwillige modelcontractvoorwaarden ontwikkelen en aanbevelen tussen aanbieders van AI-systemen met een hoog risico en derden die instrumenten, diensten, componenten of processen leveren die worden gebruikt of geïntegreerd in AI-systemen met een hoog risico, teneinde de samenwerking in de hele waardeketen te vergemakkelijken. Bij de ontwikkeling van vrijwillige modelcontractvoorwaarden moet de Commissie tevens rekening houden met de contractuele eisen die kunnen gelden in specifieke sectoren of businesscases.
- (91) Gezien de aard van AI-systemen en de risico's voor de veiligheid en de grondrechten waarmee het gebruik ervan mogelijk gepaard gaat, onder meer wat betreft de noodzaak van een behoorlijke monitoring van de prestaties van een AI-systeem in de praktijk, is het passend om specifieke verantwoordelijkheden voor gebruiksverantwoordelijken vast te stellen. Met name moeten gebruiksverantwoordelijken passende technische en organisatorische maatregelen treffen om ervoor te zorgen dat hun gebruik van AI-systemen met een hoog risico in overeenstemming is met de gebruiksaanwijzingen en voorts moeten er, waar passend, bepaalde andere verplichtingen worden vastgesteld met betrekking tot de monitoring van de werking van AI-systemen en met betrekking tot de registratie. Ook moeten gebruiksverantwoordelijken ervoor zorgen dat de personen die zijn aangewezen voor de uitvoering van de bij deze verordening vastgestelde gebruiksinstructies en menselijk toezicht, over de nodige bekwaamheid beschikken, met name over afdoende AI-geletterdheid, opleiding en autoriteit om die taken naar behoren uit te voeren. Die verplichtingen mogen geen afbreuk doen aan andere verplichtingen van gebruiksverantwoordelijken met betrekking tot AI-systemen met een hoog risico uit hoofde van het Unierecht of het nationale recht.

(92) Deze verordening doet geen afbreuk aan de verplichtingen van werkgevers op grond van het Unierecht of de nationale wetgeving en praktijk, met inbegrip van Richtlijn 2002/14/EG van het Europees Parlement en de Raad³⁹, om werknemers of hun vertegenwoordigers te informeren, of te informeren en te raadplegen, over besluiten om AI-systemen in gebruik te stellen of aan te wenden. Ook indien de voorwaarden voor deze informerings- of deze informerings- en raadplegingsverplichtingen uit hoofde van andere rechtsinstrumenten niet vervuld zijn, blijft het noodzakelijk om werknemers en hun vertegenwoordigers over het geplande inzetten van AI-systemen met een hoog risico op de werkplek te informeren. Bovendien is het recht te worden geïnformeerd aanvullend en noodzakelijk voor de aan deze verordening ten grondslag liggende doelstelling van bescherming van de grondrechten. Om die reden moet deze verordening een informeringsvereiste bevatten, die evenwel geen afbreuk mag doen aan de bestaande rechten van werknemers.

³⁹ Richtlijn 2002/14/EG van het Europees Parlement en de Raad van 11 maart 2002 tot vaststelling van een algemeen kader betreffende de informatie en de raadpleging van de werknemers in de Europese Gemeenschap (PB L 80 van 23.3.2002, blz. 29).

- (93) Hoewel aan AI-systemen verbonden risico's kunnen voortvloeien uit de manier waarop deze systemen zijn vormgegeven, kunnen de risico's ook het gevolg zijn van de manier waarop ze worden gebruikt. Gebruiksverantwoordelijken van AI-systemen met een hoog risico spelen daarom een cruciale rol bij het waarborgen van de bescherming van de grondrechten, in aanvulling op de verplichtingen van aanbieders bij de ontwikkeling van het AI-systeem. Gebruiksverantwoordelijken zijn het best in staat om te begrijpen hoe het AI-systeem met een hoog risico concreet zal worden gebruikt en kunnen derhalve potentiële aanzienlijke risico's identificeren die niet in de ontwikkelingsfase voorzien werden, want zij hebben preciezere kennis van de gebruikscontext, de personen of groepen personen die waarschijnlijk zullen worden geraakt, met inbegrip van kwetsbare groepen. De in een bijlage bij deze verordening opgenomen gebruiksverantwoordelijken van AI-systemen met een hoog risico zijn ook cruciaal voor de informering van natuurlijke personen en moeten, wanneer zij besluiten met betrekking tot natuurlijke personen nemen of helpen dergelijke besluiten te nemen, de natuurlijke personen in voorkomend geval te informeren dat zij aan het gebruik van het AI-systeem met een hoog risico zijn onderworpen. Deze informatie dient tevens het beoogde doel en het soort besluitvorming te omvatten waarvoor het systeem wordt gebruikt. De gebruiksverantwoordelijke dient de natuurlijke personen ook te informeren over hun recht op uitleg krachtens deze verordening. Als het om AI-systemen met een hoog risico gaat die voor rechtshandavingsdoeleinden worden gebruikt, moet die verplichting worden uitgevoerd overeenkomstig artikel 13 van Richtlijn (EU) 2016/680.

- (94) Elke vorm van verwerking van biometrische gegevens voor rechtshandavings-doeleinden door AI-systemen voor biometrische identificatie, moet in overeenstemming zijn met artikel 10 van Richtlijn (EU) 2016/680, op grond waarvan verwerking uitsluitend is toegestaan indien die strikt noodzakelijk is, in welk geval er passende waarborgen voor de rechten en vrijheden van de betrokkene moeten worden geboden, alsmede indien het Unierecht of het lidstatelijk recht in een dergelijke verwerking voorziet. Een dergelijk gebruik moet, indien toegestaan, tevens voldoen aan de beginselen van artikel 4, lid 1, van Richtlijn (EU) 2016/680, waaronder rechtmatigheid, billijkheid en transparantie, doelbinding, nauwkeurigheid en opslagbeperking.
- (95) Het gebruik van systemen voor biometrische identificatie op afstand achteraf moet onverminderd het toepasselijke Unierecht en dan met name Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680, gezien de indringende aard van deze systemen, worden onderworpen aan waarborgen. Systemen voor biometrische identificatie op afstand achteraf moeten te allen tijde worden gebruikt op een evenredige, legitieme en strikt noodzakelijke wijze, hetgeen betekent dat ze specifiek gericht moeten worden op de te identificeren personen en de locatie, binnen een beperkte tijdspanne, met gebruikmaking van een gesloten reeks wettelijk verkregen videobeelden. Systemen voor biometrische identificatie op afstand achteraf in het kader van rechtshandhaving mogen in geen geval gebruikt worden op een wijze die tot algemene surveillance leidt. De voorwaarden voor biometrische identificatie op afstand achteraf mogen onder geen enkel beding ruimte bieden voor omzeiling van de voorwaarden van het verbod, noch van de strikte uitzonderingen voor realtime biometrische identificatie op afstand.

- (96) Om efficiënt te waarborgen dat de grondrechten worden beschermd, moeten gebruiksverantwoordelijken van AI-systemen met een hoog risico die een publiekrechtelijk orgaan, of openbare diensten verlenende particuliere entiteiten en gebruiksverantwoordelijken van bepaalde in een bijlage bij deze verordening vermelde AI-systemen met een hoog risico, zoals bank- of verzekeringsentiteiten, een effectbeoordeling op het gebied van de grondrechten uitvoeren alvorens deze systemen in gebruik te stellen. Voor personen belangrijke diensten die van openbare aard zijn, kunnen tevens door particuliere entiteiten worden verleend. Particuliere entiteiten die dergelijke openbare diensten aanbieden, houden verband met taken van algemeen belang op het gebied van onder meer onderwijs, gezondheidszorg, sociale diensten, huisvesting en rechtsbedeling. Doel van de effectbeoordeling op het gebied van de grondrechten is dat de gebruiksverantwoordelijke de specifieke risico's voor de rechten van personen of groepen personen die waarschijnlijk zullen worden getroffen, in kaart brengt, en dat hij bepaalt welke maatregelen er nodig zijn in het geval die risico's zich voordoen. De effectbeoordeling moet worden verricht voordat het AI-systeem met een hoog risico wordt ingezet en moet worden geactualiseerd in het geval de gebruiksverantwoordelijke van mening is dat een van de relevante factoren is veranderd. De effectbeoordeling moet in kaart brengen in welke relevante processen van de gebruiksverantwoordelijke het AI-systeem met een hoog risico in overeenstemming met het beoogde doel ervan zal worden gebruikt, en moet voorts een beschrijving bevatten van de periode waarin en de frequentie waarmee het systeem zal worden gebruikt, alsmede van de specifieke categorieën natuurlijke personen en groepen die in de specifieke gebruikscontext waarschijnlijk gevolgen zullen ondervinden.

In de beoordeling moet tevens worden geïnventariseerd welke specifieke risico's op schade gevolgen kunnen hebben voor de grondrechten van die personen of groepen.

De gebruiksverantwoordelijke moet bij de beoordeling informatie gebruiken die relevant is voor een behoorlijke effectbeoordeling, waaronder door de aanbieder van het AI-systeem met een hoog risico in de gebruiksaanwijzing verstrekte informatie.

Gebruiksverantwoordelijken moeten aan de hand van de vastgestelde risico's bepalen welke maatregelen er getroffen moeten worden in het geval die risico's zich voordoen, zoals governanceregelingen in die specifieke gebruikscontext in de vorm van onder meer regelingen voor menselijk toezicht overeenkomstig de gebruiksaanwijzing of in de vorm van klachten- en beroepsprocedures, omdat deze een cruciale rol kunnen spelen bij de beperking van risico's voor de grondrechten in concrete gebruikgevallen. Na uitvoering van die effectbeoordeling moet de gebruiksverantwoordelijke de relevante markttoezichtautoriteit daarvan in kennis stellen. Gebruiksverantwoordelijken van AI-systemen met een hoog risico kunnen bij de uitvoering van de effectbeoordeling en het ontwerpen van maatregelen voor het geval de risico's werkelijkheid worden, met name bij gebruik van AI-systemen in de publieke sector, zich voor de inwinning van relevante informatie voor de effectbeoordeling in voorkomend geval tot relevante belanghebbenden wenden, zoals de vertegenwoordigers van groepen personen die waarschijnlijk gevolgen van het AI-systeem zullen ondervinden, alsmede tot onafhankelijke deskundigen en maatschappelijke organisaties. Het Europees Bureau voor artificiële intelligentie ("AI-bureau") moet een model-vragenlijst ontwikkelen om naleving te vergemakkelijken en de administratieve lasten voor gebruiksverantwoordelijken te verminderen.

- (97) Het begrip “AI-model voor algemene doeleinden” moet met het oog op de rechtszekerheid duidelijk worden gedefinieerd en worden gescheiden van het begrip “AI-systeem”. De definitie moet gebaseerd zijn op de belangrijkste eigenschappen en kenmerken van AI-modellen voor algemene doeleinden, met name het algemene karakter en het vermogen om op competente wijze een breed scala aan onderscheiden taken uit te voeren. Dit soort modellen wordt getraind met grote hoeveelheden gegevens, via uiteenlopende methoden als self-supervised, unsupervised of reinforcement learning. AI-modellen voor algemene doeleinden kunnen op verschillende manieren in de handel worden gebracht, onder meer via bibliotheken en applicatie-programma-interfaces (API’s), of als rechtstreekse download of fysieke kopie. Deze modellen kunnen nader worden gewijzigd of verfijnd tot nieuwe modellen. AI-modellen zijn weliswaar een essentieel onderdeel van AI-systemen, maar vormen geen AI-systemen op zich. Om een AI-systeem te worden, moeten er aan AI-modellen nog andere componenten worden toegevoegd, bijvoorbeeld een gebruikersinterface. AI-modellen worden doorgaans geïntegreerd in en vormen een onderdeel van AI-systemen. Deze verordening voorziet in specifieke regels voor AI-modellen voor algemene doeleinden en voor AI-modellen voor algemene doeleinden die systeemrisico’s inhouden, hetgeen ook van toepassing dient te zijn als deze modellen geïntegreerd zijn in of deel uitmaken van een AI-systeem. De verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden behoren van toepassing te zijn zodra een AI-model voor algemene doeleinden in de handel wordt gebracht.

In het geval een aanbieder van een AI-model voor algemene doeleinden in een eigen AI-systeem dat op de markt wordt aangeboden of in gebruik wordt gesteld, een eigen model integreert, moet dat model worden geacht in de handel te zijn gebracht en dienen de verplichtingen krachtens deze verordening voor modellen derhalve van toepassing blijven naast die voor AI-systemen. De verplichtingen voor modellen behoren evenwel niet van toepassing te zijn indien een eigen model gebruikt wordt voor zuiver interne processen die niet essentieel zijn voor de levering van een product of een dienst aan derden en indien er geen rechten van natuurlijke personen in het geding zijn. AI-modellen voor algemene doeleinden met een systeemrisico moeten gezien hun in potentie aanzienlijk negatieve effecten altijd onderworpen zijn aan de relevante verplichtingen uit hoofde van deze verordening. De definitie mag geen betrekking hebben op AI-modellen die louter voor onderzoeks-, ontwikkelings- en prototypingdoeleinden worden gebruikt alvorens zij in de handel worden gebracht. Dit laat onverlet dat eenmaal een model na gebruik voor voornoemde doeleinden in de handel wordt gebracht, aan deze verordening moet worden voldaan.

- (98) Hoewel het algemene karakter van een model, onder meer, ook aan de hand van het aantal parameters kan worden bepaald, moeten modellen met ten minste een miljard parameters die via grootschalig self-supervised leren getraind zijn met grote hoeveelheden gegevens, geacht worden een aanzienlijke algemeenheid te vertonen en op competente wijze een breed scala aan onderscheidende taken te kunnen uitvoeren.
- (99) Grote generatieve AI-modellen zijn een typisch voorbeeld van AI-modellen voor algemene doeleinden, aangezien ze op flexibele wijze content kunnen genereren in de vorm van bijvoorbeeld tekst, audio, beelden of video, waarmee eenvoudig een breed scala aan onderscheiden taken kan worden uitgevoerd.

- (100) Indien een AI-model voor algemene doeleinden is geïntegreerd in of deel uitmaakt van een AI-systeem, moet dit systeem als AI-systeem voor algemene doeleinden worden aangemerkt indien het dankzij deze integratie aangewend kan worden voor uiteenlopende doeleinden. Een AI-systeem voor algemene doeleinden kan rechtstreeks worden gebruikt of kan worden geïntegreerd in meerdere andere AI-systemen.
- (101) Aanbieders van AI-modellen voor algemene doeleinden hebben een bijzondere rol en verantwoordelijkheid binnen de AI-waardeketen, aangezien de modellen die zij leveren de basis kunnen vormen voor een reeks systemen verder in de AI-waardeketen, veelal aangeboden door aanbieders verder in de AI-waardeketen, hetgeen om een goed inzicht in de modellen en hun capaciteiten vraagt, zowel qua integratie van de modellen in hun producten als qua naleving van hun verplichtingen uit hoofde van deze of andere verordeningen. Er zijn derhalve evenredige transparantiemaatregelen nodig, zoals opstelling en bijwerking van documentatie en verstrekking van informatie over het AI-model voor algemeen gebruik door de aanbieders verder in de AI-waardeketen. De aanbieder van het AI-model voor algemene doeleinden dient technische documentatie op te stellen en bij te werken om deze op verzoek te kunnen overleggen aan het AI-bureau en de nationale bevoegde autoriteiten. De minimaal in de documentatie op te nemen elementen moeten worden vastgelegd in specifieke bijlagen bij deze verordening. De Commissie moet de bevoegdheid krijgen om die bijlagen in het licht van de technologische ontwikkelingen bij gedelegeerde handelingen te wijzigen.

- (102) Software en gegevens, met inbegrip van modellen, vrijgegeven in het kader van een vrije en opensourcelicentie op basis waarvan ze vrijelijk kunnen worden gedeeld en gebruikers ze in al dan niet gewijzigde vorm vrijelijk kunnen raadplegen, gebruiken, wijzigen en herdistribueren, kunnen bijdragen tot onderzoek en innovatie op de markt en aanzienlijke groeikansen bieden voor de economie van de Unie. In het kader van vrije en opensourcelicenties vrijgegeven AI-modellen voor algemene doeleinden moeten worden aangemerkt als hoge transparantie en openheid waarborgend, indien de parameters ervan, met inbegrip van de wegingen, de informatie over de modelarchitectuur en de informatie over het gebruik van het model, openbaar worden gemaakt. Een licentie moet eveneens als vrij en open source worden aangemerkt ingeval gebruikers op basis ervan software en gegevens kunnen exploiteren, kopiëren, verspreiden, bestuderen, wijzigen en verbeteren, met inbegrip van modellen, mits de oorspronkelijke aanbieder van het model vermeld wordt en er identieke of vergelijkbare distributievoorwaarden in acht worden genomen.
- (103) “Vrije en opensource-AI-componenten” staat voor de software en de gegevens, met inbegrip van de modellen en AI-modellen, -instrumenten, -diensten of -processen voor algemene doeleinden van een AI-systeem. Vrije en opensource-AI-componenten kunnen via verschillende kanalen worden aangeboden, inclusief via ontwikkeling op open dataopslagplaatsen. AI-componenten die worden verstrekt tegen betaling of anderszins te gelde worden gemaakt via onder meer verlening van technische ondersteuning of andere diensten met betrekking tot de AI-component, waaronder op een softwareplatform, of via het gebruik van persoonsgegevens om andere redenen dan uitsluitend ter verbetering van de beveiliging, compatibiliteit of interoperabiliteit van de software, met uitzondering van transacties tussen micro-ondernemingen, mogen voor de toepassing van deze verordening niet in aanmerking komen voor de uitzonderingen op vrije en opensource-AI-componenten. Het loutere beschikbaar stellen van AI-componenten via open registers mag niet als tegeldemaking worden aangemerkt.

- (104) De aanbieders van AI-modellen voor algemene doeleinden die worden vrijgegeven in het kader van een vrije en opensource-licentie en waarvan de parameters, met inbegrip van de wegingen, de informatie over de modelarchitectuur en de informatie over het gebruik van het model, openbaar worden gemaakt, moeten worden onderworpen aan uitzonderingen met betrekking tot de transparantievereisten voor AI-modellen voor algemene doeleinden, tenzij zij geacht kunnen worden een systeemrisico te vertegenwoordigen. In dat geval mag de omstandigheid dat het model transparant is en vergezeld gaat van een opensource-licentie niet als voldoende reden worden aangemerkt om de verplichtingen uit hoofde van deze verordening niet na te leven. Aangezien het geen vanzelfsprekendheid is dat er bij de beschikbaarstelling van AI-modellen voor algemene doeleinden middels vrije en opensource-licenties substantiële informatie beschikbaar komt over de voor de training of verfijning van het model gebruikte datasets of over de wijze waarop daarbij gezorgd is voor naleving van het auteursrecht, mag de uitzondering voor AI-modellen voor algemene doeleinden wat betreft de naleving van de transparantievereisten in elk geval geen betrekking hebben op de verplichting om een samenvatting op te stellen van de content die voor de training van het model is gebruikt en ook niet op de verplichting tot invoering van een beleid ter naleving van het Unierecht inzake auteursrechten en dan met name ter vaststelling en naleving van het voorbehoud van rechten op grond van artikel 4, lid 3, van Richtlijn (EU) 2019/790 van het Europees Parlement en de Raad⁴⁰.

⁴⁰ Richtlijn (EU) 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG, PB L 130 van 17.5.2019, blz. 92.

- (105) AI-modellen voor algemeen gebruik, met name grote generatieve AI-modellen, die tekst, beelden en andere content kunnen genereren, bieden unieke innovatiemogelijkheden, maar leiden ook tot uitdagingen voor kunstenaars, auteurs en andere makers en de manier waarop hun creatieve content wordt gecreëerd, verspreid, gebruikt en geconsumeerd. Voor de ontwikkeling en opleiding van dergelijke modellen is toegang nodig tot enorme hoeveelheden tekst, afbeeldingen, video's en andere data. In dit verband kan voor het vergaren en analyseren van die mogelijkwerwijs door het auteursrecht en naburige rechten beschermde content, op grote schaal tekst- en dataminingtechnieken worden gebruikt. Voor elk gebruik van auteursrechtelijk beschermde content is toestemming van de betrokken rechthebbende vereist, tenzij er relevante uitzonderingen en beperkingen op het auteursrecht gelden. Bij Richtlijn (EU) 2019/790 zijn uitzonderingen en beperkingen ingevoerd die onder bepaalde voorwaarden toestaan dat werken of andere materialen voor doeleinden van tekst- en datamining worden gereproduceerd of geëxtraheerd. Op grond van deze regels kunnen rechthebbenden ervoor kiezen hun rechten op hun werken of andere materialen voor te behouden teneinde tekst- en datamining te voorkomen, tenzij dit gebeurt voor doeleinden van wetenschappelijk onderzoek. Indien opt-outrechten uitdrukkelijk en op passende wijze zijn voorbehouden, dient een aanbieder van AI-modellen voor algemene doeleinden indien hij de werken voor tekst- en datamining wil gebruiken, toestemming aan de rechthebbenden te vragen.

- (106) Aanbieders die AI-modellen voor algemene doeleinden in de Unie in de handel brengen, zijn gehouden de naleving van de desbetreffende verplichtingen in deze verordening te waarborgen. Zij moeten daartoe een beleid invoeren ter naleving van het Unierecht inzake auteursrechten en naburige rechten, met name om kennis te hebben van het door rechthebbenden geuite voorbehoud van rechten op grond van artikel 4, lid 3, van Richtlijn (EU) 2019/790 en dit na te leven. Aanbieders die in de Unie een AI-model voor algemene doeleinden in de handel brengen, zijn hiertoe verplicht, ongeacht de jurisdictie waarin de auteursrechtelijke relevante handelingen plaatsvinden die helpen die AI-modellen voor algemene doeleinden te trainen. Alleen op deze manier kan gezorgd worden voor een gelijk speelveld voor aanbieders van AI-modellen voor algemene doeleinden, waar geen enkele aanbieder zich een concurrentievoordeel op de Uniemarkt mag kunnen verschaffen met lagere auteursrechtelijke normen dan de in de Unie toepasselijke normen.

- (107) Voor een grotere transparantie ten aanzien van de bij de pre-training en training van AI-modellen voor algemene doeleinden gebruikte data, met inbegrip van door het auteursrecht beschermde tekst en data, is het passend dat aanbieders van dergelijke modellen een voldoende gedetailleerde samenvatting maken en publiceren van de voor de training van het AI-model voor algemene doeleinden gebruikte content. Terdege rekening houdend met de noodzaak tot bescherming van bedrijfsgeheimen en vertrouwelijke bedrijfsinformatie moet deze samenvatting breed van karakter zijn in plaats van technisch gedetailleerd, teneinde partijen met legitieme belangen, waaronder houders van auteursrechten, in staat te stellen hun rechten uit hoofde van het Unierecht uit te oefenen en te handhaven. Zo kan er bijvoorbeeld een opsomming worden gegeven van de belangrijkste gegevensverzamelingen of -reeksen waarmee het model is getraind, zoals grote particuliere of openbare databanken of gegevensarchieven, en kan een uitleg in de vorm van een relaas worden gegeven over andere gebruikte gegevensbronnen. Het is passend dat het AI-bureau een model voor die samenvatting verstrekt, dat een eenvoudig en doeltreffend model dient te zijn waarmee de aanbieder de vereiste samenvatting in de vorm van een relaas verstrekken kan.
- (108) Wat betreft de verplichtingen van aanbieders van AI-modellen voor algemene doeleinden om een beleid in te voeren om aan het recht van de Unie inzake auteursrecht te voldoen en om een samenvatting van de voor de training gebruikte content te publiceren, moet het AI-bureau controleren of de aanbieder aan die verplichtingen voldoet, zonder evenwel geval voor geval de trainingsdata te controleren of te beoordelen qua naleving van het auteursrecht. Deze verordening doet geen afbreuk aan de handhaving van de auteursrechtregels krachtens het Unierecht.

- (109) De naleving van de verplichtingen van aanbieders van AI-modellen voor algemene doeleinden moet evenredig zijn aan en in verhouding staan tot het soort modelaanbieder, waarbij personen die modellen ontwikkelen of gebruiken voor niet-professioneel of wetenschappelijk onderzoek, van de verplichtingen zijn uitgesloten maar wel moeten worden aangemoedigd deze verplichtingen vrijwillig te omarmen. Onverminderd het recht van de Unie inzake auteursrechten moet qua naleving van die verplichtingen terdege rekening worden gehouden met de omvang van de aanbieder en moeten er voor kmo's, waaronder start-ups, vereenvoudigde wijzen van naleving mogelijk zijn die geen buitensporige kosten mogen meebrengen en het gebruik van dergelijke modellen niet mogen ontmoedigen. Bij wijziging of verfijning van een model moeten de verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden beperkt blijven tot die wijziging of verfijning, bijvoorbeeld door voor te schrijven dat de reeds bestaande technische documentatie louter aangevuld wordt met informatie over de wijzigingen, met inbegrip van nieuwe trainingsdatabronnen, als middel om te voldoen aan de waardeketenverplichtingen krachtens deze verordening.

- (110) AI-modellen voor algemene doeleinden kunnen systeemrisico's met zich meebrengen, waaronder feitelijke of redelijkerwijs te voorziene negatieve effecten die verband houden met zware ongevallen, verstoringen van kritieke sectoren en ernstige gevolgen voor de volksgezondheid en de openbare veiligheid, allerhande feitelijke of redelijkerwijs voorzienbare negatieve effecten op democratische processen en de openbare en economische veiligheid, alsmede de verspreiding van illegale, valse of discriminerende content. Systeemrisico's nemen logischerwijs toe naargelang de capaciteiten en het bereik van een model groter zijn, kunnen zich voordoen gedurende de gehele levenscyclus van het model en worden beïnvloed door elementen als misbruik van het model, de betrouwbaarheid, billijkheid, beveiliging en mate van autonomie ervan, alsmede door de toegang van het model tot instrumenten, nieuwe of gecombineerde modaliteiten, introductie- en distributiestrategieën, en door het potentieel om waarborgen te omzeilen en andere factoren. Internationaal is bij de aanpak van de problematiek tot dusver met name gebleken dat aandacht moet worden besteed aan de risico's die voortvloeien uit mogelijk opzettelijk misbruik of uit onbedoelde problemen met de controle op de afstemming op wat de mens met het model beoogt; chemische, biologische, radiologische en nucleaire risico's, zoals de manieren waarop belemmeringen op de toegang kunnen worden verlaagd, onder meer voor doeleinden van wapenontwikkeling, van verwerving van wapenontwerpen, en van wapengebruik; offensieve cybercapaciteiten, zoals manieren om kwetsbaarheden op te sporen, te exploiteren of operationeel te gebruiken; de effecten van interactie en het gebruik van instrumenten, waaronder bijvoorbeeld de capaciteit om fysieke systemen te controleren en kritieke infrastructuur te verstoren; het risico dat modellen kopieën van zichzelf maken, zichzelf repliceren, of andere modellen trainen; de manieren waarop modellen kunnen leiden tot schadelijke vooringenomenheid en discriminatie, met alle risico's voor individuen, gemeenschappen of samenlevingen van dien; de facilitering van desinformatie of privacyschendingen die een bedreiging vormen voor de democratische rechtsorde en de mensenrechten; het risico dat een bepaalde gebeurtenis kan leiden tot een kettingreactie met aanzienlijke negatieve effecten op een hele stad, een heel vakgebied of een hele gemeenschap.

- (111) Het strekt tot aanbeveling een methodiek te ontwikkelen voor de classificatie van AI-modellen voor algemene doeleinden als AI-model voor algemene doeleinden met een systeemrisico. Systeemrisico's zijn het gevolg van bijzonder hoge capaciteiten, reden waarom een AI-model voor algemene doeleinden geacht moet worden systeemrisico's te vertegenwoordigen indien het capaciteiten met een grote impact heeft, dewelke als zodanig wordt vastgesteld op basis van passende technische instrumenten en methodieken, of indien het vanwege zijn bereik aanzienlijke gevolgen heeft voor de interne markt.
- “Capaciteiten met een grote impact” in AI-modellen voor algemene doeleinden: capaciteiten die overeenkomen met of groter zijn dan de capaciteiten die worden opgetekend bij de meest geavanceerde AI-modellen voor algemene doeleinden; Het volledige scala aan mogelijkheden binnen een model wordt pas duidelijker eenmaal het in de handel is gebracht of gebruiksverantwoordelijken met het model werken. Volgens de stand van de techniek op het moment van inwerkingtreding van deze verordening is de voor de training van het AI-model voor algemene doeleinden gebruikte cumulatieve rekeninput, gemeten in zwevendekomma bewerkingen, een van de relevante benaderingen voor modelcapaciteiten. De voor het trainen gebruikte cumulatieve rekeninput bevat het totaal aan voor de activiteiten en methoden ter verbetering van de capaciteiten van het model gebruikte rekeninput voorafgaand aan het inzetten ervan, zoals pre-training, het genereren van synthetische gegevens en verfijning. Er moet derhalve een initiële drempel voor zwevendekomma bewerkingen worden vastgesteld, die, indien een AI-model voor algemene doeleinden daaraan voldoet, leidt tot de aanname dat het model een AI-model voor algemene doeleinden met systeemrisico's is. Deze drempel moet in de loop van de tijd worden aangepast aan de technologische en industriële vooruitgang, zoals betere algoritmes of efficiëntere hardware, en moet worden aangevuld met modelcapaciteit-benchmarks en -indicatoren.

Om deze vooruitgang te kennen, moet het AI-bureau samenwerken met de wetenschappelijke gemeenschap, het bedrijfsleven, het maatschappelijk middenveld en andere deskundigen. Drempelwaarden en ook instrumenten en benchmarks ter beoordeling van capaciteiten met een grote impact, moeten gedegen kunnen voorspellen in hoeverre een AI-model voor algemene doeleinden van algemene aard is, wat de capaciteiten ervan zijn en welk systeemrisico aan het model kleeft. Daarnaast zouden de drempelwaarden en de instrumenten en benchmarks ter beoordeling van capaciteiten met een grote impact, rekening kunnen houden met de wijze waarop het model in de handel zal worden gebracht of het aantal gebruikers waarvoor het gevolgen kan hebben. Ter aanvulling van dit systeem moet de Commissie de mogelijkheid hebben om individuele besluiten te nemen tot aanmerking van een dergelijk model als AI-model voor algemene doeleinden met een systeemrisico, in het geval wordt vastgesteld dat een AI-model voor algemene doeleinden mogelijkheden of een effect heeft dat gelijkwaardig is aan die welke onder de vastgestelde drempel vallen. Dat besluit moet worden genomen op basis van een algemene beoordeling van de in een bijlage bij deze verordening vastgestelde criteria voor de aanwijzing van een AI-model voor algemene doeleinden met een systeemrisico, zoals de kwaliteit of omvang van de trainingsdataset, het aantal zakelijke en eindgebruikers van het model, de input- en outputmodaliteiten ervan, de mate van autonomie en schaalbaarheid ervan, of de instrumenten waartoe het toegang heeft. Als een aanbieder wiens model is aangewezen als AI-model voor algemene doeleinden met een systeemrisico een met redenen omkleed verzoek indient, dient de Commissie daarmee rekening te houden en kan zij besluiten opnieuw te beoordelen of het AI-model voor algemene doeleinden nog steeds wordt beschouwd als een AI-model dat systeemrisico's vertoont.

(112) Het is tevens noodzakelijk tot een procedure te komen voor de classificatie van AI-modellen voor algemene doeleinden met een systeemrisico. Een AI-model voor algemeen gebruik dat aan de toepasselijke drempel voor capaciteiten met een grote impact voldoet, dient als AI-model voor algemene doeleinden met een systeemrisico te worden aangemerkt. De aanbieder behoort uiterlijk twee weken nadat aan de vereisten is voldaan of nadat bekend is geworden dat een AI-model voor algemene doeleinden voldoet aan de vereisten die tot het vermoeden leiden, het AI-bureau daarvan in kennis te stellen. Dit is met name relevant met betrekking tot de drempel van zwevendekomma bewerkingen, omdat de training van AI-modellen voor algemene doeleinden uitgebreide planning vergt met onder meer voorafgaande toewijzing van rekeninputmiddelen, waardoor aanbieders van AI-modellen voor algemene doeleinden reeds vóór voltooiing van de training weten kunnen of hun model aan de drempel zal voldoen. In het kader van die kennisgeving moet de aanbieder kunnen aantonen dat een AI-model voor algemene doeleinden dankzij zijn specifieke kenmerken bij wijze van uitzondering geen systeemrisico's met zich meebrengt en dat het dus niet als AI-model voor algemene doeleinden met systeemrisico's mag worden aangemerkt. Het AI-bureau kan dankzij die informatie anticiperen op het in de handel brengen van AI-modellen voor algemene doeleinden met systeemrisico's, en de aanbieders kunnen reeds in een vroeg stadium met het AI-bureau in contact treden. Die informatie is met name van belang met betrekking tot AI-modellen voor algemene doeleinden waarvan het de bedoeling is deze als open source vrij te geven, want eenmaal als het opensourcemodel is vrijgegeven, kan het moeilijker zijn de nodige maatregelen ter naleving van de verplichtingen uit hoofde van deze verordening te treffen.

- (113) Indien de Commissie kennis krijgt van het feit dat een AI-model voor algemene doeleinden voldoet aan de vereisten om als AI-model voor algemene doeleinden met een systeemrisico te worden aangemerkt, terwijl dat eerder niet bekend was of de betrokken aanbieder de Commissie kennisgeving had gedaan, moet de Commissie de bevoegdheid hebben dit model alsnog als zodanig aan te merken. Naast de monitoringactiviteiten van het AI-bureau moet er een systeem van gekwalificeerde waarschuwingen komen dat ervoor zorgt dat het AI-bureau door het wetenschappelijk panel in kennis wordt gesteld van AI-modellen voor algemene doeleinden die mogelijk als AI-modellen voor algemene doeleinden met een systeemrisico moeten worden geclassificeerd.
- (114) De aanbieders van AI-modellen voor algemene doeleinden die systeemrisico's inhouden, moeten, naast de verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden, onderworpen worden aan verplichtingen die gericht zijn op het identificeren en beperken van die risico's en op waarborging van een passend niveau van cyberbeveiliging, ongeacht of het model een op zichzelf staand model is of ingebed in een AI-systeem of in een product. Aanbieders moeten met het oog op verwezenlijking van deze doelstellingen, bij deze verordening verplicht worden de nodige modevaluaties uit te voeren, met name voordat een model voor het eerst in de handel wordt gebracht, in het kader waarvan onder meer tests gericht op het ontdekken van kwetsbaarheden in het model moeten worden uitgevoerd, alsmede, in voorkomend geval, uiteenlopende interne of onafhankelijke externe tests. Daarnaast moeten aanbieders van AI-modellen voor algemene doeleinden met systeemrisico's die systeemrisico's voortdurend analyseren en binnen de perken houden via onder meer beleid voor risicobeheer in de vorm van bijvoorbeeld verantwoordings- en governanceprocessen, monitoring na het in de handel brengen van het model, passende maatregelen gedurende de gehele levenscyclus, en samenwerking met relevante actoren in de AI-waardeketen.

- (115) Aanbieders van AI-modellen voor algemene doeleinden met systeemrisico's dienen mogelijke systeemrisico's te beoordelen en te beperken. Indien er zich als gevolg van de ontwikkeling of het gebruik van een AI-model voor algemene doeleinden die systeemrisico's kan inhouden een ernstig incident voordoet, ondanks inspanningen om met het model verband houdende risico's te identificeren en te voorkomen, moet de aanbieder van het AI-model voor algemene doeleinden onverwijld het verdere verloop van het incident beginnen te volgen en de Commissie en de nationale bevoegde autoriteiten alle relevante informatie en mogelijke corrigerende maatregelen melden. Bovendien moeten aanbieders zorgen voor een passend niveau van cyberbeveiliging voor het model en de fysieke infrastructuur ervan, indien van toepassing, gedurende de gehele levenscyclus van het model. Bij de cyberbeveiliging in verband met systeemrisico's als gevolg van kwaadwillig gebruik of aanvallen, moet terdege rekening worden gehouden met onopzettelijke modellekken, ongeoorloofde vrijgave, omzeiling van veiligheidsmaatregelen, alsmede met bescherming tegen cyberaanvallen, ongeoorloofde toegang, en modeldiefstal. Die bescherming kan worden geboden door modelwegingen, algoritmen, servers en datasets te beveiligen, bijvoorbeeld met operationele beveiligingsmaatregelen voor informatie, specifiek cyberbeveiligingsbeleid, passende technische en bewezen oplossingen, alsmede met controles op cyber- en fysieke toegang, afgestemd op de relevante omstandigheden en risico's.

- (116) Het AI-bureau moet de opstelling, evaluatie en aanpassing van praktijkcodes aanmoedigen en vergemakkelijken, rekening houdend met internationale manieren van aanpak. Alle aanbieders van AI-modellen voor algemene doeleinden kunnen worden uitgenodigd eraan deel te nemen. Om ervoor te zorgen dat de praktijkcodes aansluiten op de stand van de techniek en ze terdege rekening houden met een brede waaier aan perspectieven, moet het AI-bureau samenwerken met de relevante nationale bevoegde autoriteiten en kan het, in voorkomend geval, ter opstelling van de praktijkcodes overleg voeren met maatschappelijke organisaties en andere relevante belanghebbenden en deskundigen, waaronder het wetenschappelijk panel. De praktijkcodes moeten betrekking hebben op verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden en van AI-modellen voor algemene doeleinden die systeemrisico's inhouden. Wat systeemrisico's betreft, moeten praktijkcodes bovendien bijdragen tot de vaststelling van een taxonomie van de soorten systeemrisico's op het niveau van de Unie, voorzien van de kenmerken en bronnen van deze risico's. Voorts moeten praktijkcodes gericht zijn op specifieke risicobeoordelings- en risicobeperkende maatregelen.

- (117) De praktijkcodes moeten een centraal instrument zijn voor de correcte naleving van de verplichtingen van aanbieders van AI-modellen voor algemene doeleinden uit hoofde van deze verordening. Aanbieders moeten voor het staven van hun naleving van de verplichtingen kunnen vertrouwen op praktijkcodes. De Commissie kan bij uitvoeringshandelingen een gedragscode vaststellen en deze binnen de Unie een algemene geldigheid verlenen, of anderszins gemeenschappelijke regels vaststellen voor de uitvoering van de desbetreffende verplichtingen, indien er op het moment dat deze verordening van toepassing wordt nog geen gedragscode voorhanden is of het AI-bureau de wel reeds voorhanden zijnde gedragscode ontoereikend acht. Zodra een geharmoniseerde norm gepubliceerd is en het AI-bureau deze in het licht van de relevante verplichtingen geschikt heeft bevonden, moet naleving van een Europese geharmoniseerde norm aanbieders het vermoeden van conformiteit bieden. Aanbieders van AI-modellen voor algemene doeleinden moeten ook met alternatieve geschikte middelen kunnen aantonen dat zij aan de relevante verplichtingen voldoen in het geval er geen praktijkcodes of geharmoniseerde normen beschikbaar zijn, of wanneer zij ervoor kiezen geen beroep op die codes of normen te doen.

- (118) Deze verordening reguleert AI-systemen en AI-modellen door relevante marktdeelnemers die deze in de Unie in de handel brengen, in gebruik stellen of in gebruik nemen bepaalde eisen en verplichtingen op te leggen, en vormt een aanvulling op de verplichtingen voor aanbieders van tussenhandelsdiensten die dit soort systemen of modellen in hun bij Verordening (EU) 2022/2065 gereguleerde diensten integreren. Voor zover dergelijke systemen of modellen zijn ingebed in als zeer groot aangemerkte onlineplatforms of onlinezoekmachines, vallen zij onder het kader voor risicobeheer krachtens Verordening (EU) 2022/2065. Bijgevolg moeten de overeenkomstige verplichtingen van deze verordening als vervuld worden beschouwd, tenzij er in dergelijke modellen aanzienlijke systeemrisico's worden geconstateerd die niet onder Verordening (EU) 2022/2065 vallen. Binnen dit kader zijn aanbieders van zeer grote onlineplatforms en zeer grote onlinezoekmachines verplicht te beoordelen welke systeemrisico's er potentieel uit het ontwerp, de werking en het gebruik van hun diensten voortvloeien, met inbegrip van de wijze waarop het ontwerp van de in de dienst gebruikte algoritmische systemen die tot dergelijke risico's kunnen bijdragen, alsmede welke systeemrisico's er kunnen optreden bij misbruik. Deze aanbieders zijn ook verplicht passende risicobeperkende maatregelen te treffen, met inachtneming van de grondrechten.

- (119) Gezien het snelle innovatietempo en de technologische ontwikkeling van de digitale diensten die onder het toepassingsgebied van verschillende Unierechtelijke instrumenten vallen en met name rekening houdend met het gebruik en de perceptie van de afnemers van die diensten, kunnen de onder deze verordening vallende AI-systemen worden aangeboden als tussenhandelsdiensten of delen daarvan in de zin van Verordening (EU) 2022/2065, die op technologie-neutrale wijze moet worden geïnterpreteerd. AI-systemen kunnen bijvoorbeeld worden gebruikt om onlinezoekmachines aan te bieden, en wel dusdanig dat een AI-systeem zoals een online chatbot in beginsel alle websites doorzoekt, om de zoekresultaten vervolgens in zijn bestaande kennis op te nemen en dan de bijgewerkte kennis te gebruiken voor het genereren van één enkele output waarin informatie uit verschillende bronnen wordt gecombineerd.
- (120) Voorts zijn de verplichtingen die in deze verordening aan aanbieders en gebruiksverantwoordelijken van bepaalde AI-systemen worden opgelegd om opsporing mogelijk te maken, evenals de bekendmaking dat de outputs van die systemen kunstmatig worden gegenereerd of gemanipuleerd, bijzonder relevant voor het vergemakkelijken van de doeltreffende uitvoering van Verordening (EU) 2022/2065. Dit geldt met name voor de verplichtingen van aanbieders van zeer grote onlineplatforms of zeer grote onlinezoekmachines om systeemrisico's die kunnen voortvloeien uit de verspreiding van kunstmatig gegenereerde of gemanipuleerde content te identificeren en te beperken, en dan met name het risico op feitelijke of voorzienbare negatieve effecten op democratische processen, het maatschappelijk debat en verkiezingsprocessen, onder meer van desinformatie.

(121) Normalisatie moet een belangrijke rol spelen bij de levering van technische oplossingen aan aanbieders om de naleving van deze verordening te waarborgen, in overeenstemming met de stand van de techniek, opdat de innovatie, het concurrentievermogen en ook de groei op de eengemaakte markt kunnen worden bevorderd. De naleving van geharmoniseerde normen, zoals gedefinieerd in artikel 2, lid 1, punt c), van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad⁴¹, die normaal gesproken de stand van de techniek moet weerspiegelen, moet een middel zijn voor aanbieders om de overeenstemming met de voorschriften van deze verordening aan te tonen. Het is daarom zaak aan te sturen op evenwichtige belangenvertegenwoordiging door overeenkomstig de artikelen 5 en 6 van Verordening (EU) nr. 1025/2012 alle relevante belanghebbenden te betrekken bij de ontwikkeling van normen, met name kmo's, consumentenorganisaties en belanghebbenden op sociaal gebied en dat van milieu. De Commissie moet voor een soepelere naleving de normalisatieverzoeken zonder onnodige vertraging afgeven. Bij het opstellen van normalisatieverzoeken moet de Commissie de nodige expertise inwinnen bij het adviesforum voor AI en de AI-board. Bij ontstentenis van relevante verwijzingen naar geharmoniseerde normen moet de Commissie evenwel gemeenschappelijke specificaties voor bepaalde eisen uit hoofde van deze verordening kunnen vaststellen, bij uitvoeringshandeling en na raadpleging van het adviesforum.

⁴¹ Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

De gemeenschappelijke specificaties moeten een uitzonderlijke achtervang zijn om de aanbieder te kunnen laten voldoen aan de eisen van deze verordening ingeval het normalisatieverzoek door geen van de Europese normalisatieorganisaties is aanvaard, ingeval de relevante geharmoniseerde normen onvoldoende tegemoetkomen aan problemen op het gebied van de grondrechten, ingeval de geharmoniseerde normen niet aan het verzoek voldoen, of ingeval er vertraging is ontstaan bij de vaststelling van een passende geharmoniseerde norm. Indien een dergelijke vertraging bij de vaststelling van een geharmoniseerde norm te wijten is aan de technische complexiteit van die norm, moet de Commissie hier rekening mee houden alvorens te overwegen gemeenschappelijke specificaties vast te stellen. De Commissie wordt aangemoedigd om bij de ontwikkeling van gemeenschappelijke specificaties samen te werken met internationale partners en internationale normalisatie-instellingen.

- (122) Het is onverminderd het gebruik van geharmoniseerde normen en gemeenschappelijke specificaties passend dat aanbieders van een AI-systeem met een hoog risico dat getraind en getest is op data met betrekking tot de specifieke geografische, gedrags-, contextuele of functionele omgeving waarin het de bedoeling is het systeem te gebruiken, verondersteld worden aan de desbetreffende maatregel krachtens de bij deze verordening vastgestelde datagovernancevereiste te voldoen. Onverminderd de bij deze verordening vastgestelde vereisten met betrekking tot robuustheid en nauwkeurigheid, moeten overeenkomstig artikel 54, lid 3, van Verordening (EU) 2019/881, gecertificeerde AI-systemen met een hoog risico of AI-systemen met een hoog risico waarvoor in het kader van een cyberbeveiligingsregeling uit hoofde van die verordening een conformiteitsverklaring is afgegeven en waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, worden geacht aan het cyberbeveiligingsvereiste van deze verordening te voldoen, voor zover het cyberbeveiligingscertificaat of de conformiteitsverklaring of delen daarvan het cyberbeveiligingsvereiste van deze verordening bestrijken. Dit doet geen afbreuk aan het vrijwillige karakter van die cyberbeveiligingsregeling.
- (123) Om te zorgen voor een hoog niveau van betrouwbaarheid van AI-systemen met een hoog risico, moeten deze systemen worden onderworpen aan een conformiteitsbeoordeling voordat zij in de handel worden gebracht of in gebruik worden gesteld.

- (124) Teneinde de lasten voor operatoren tot een minimum te beperken en eventuele mogelijke overlappingsen te voorkomen, moet de overeenstemming van AI-systemen met een hoog risico die verband houden met producten die vallen onder bestaande harmonisatiewetgeving van de Unie volgens het nieuwe wetgevingskader met de voorschriften van deze verordening, worden beoordeeld als onderdeel van de conformiteitsbeoordeling waarin bij die wetgeving reeds is voorzien. De toepasselijkheid van de voorschriften van deze verordening mag dus geen gevolgen hebben voor de specifieke logica, methode of algemene structuur van de conformiteitsbeoordeling uit hoofde van de desbetreffende harmonisatiewetgeving van de Unie.
- (125) Gezien de complexiteit van AI-systemen met een hoog risico en de aan die systemen verbonden risico's, is het belangrijk een adequate conformiteitsbeoordelingsprocedure voor AI-systemen met een hoog risico te ontwikkelen en daar aangemelde instanties bij te betrekken, de zogeheten conformiteitsbeoordeling door derden. Gezien de huidige ervaring van personen die professionele certificeringen vóór het in de handel brengen uitvoeren op het gebied van productveiligheid en de andere aard van de risico's waarmee dat gepaard gaat, is het echter passend om, in ieder geval in een eerste fase van de toepassing van deze verordening, het toepassingsgebied van conformiteitsbeoordelingen door derden van AI-systemen met een hoog risico die geen verband houden met producten, te beperken. Daarom moet de conformiteitsbeoordeling van dergelijke systemen in de regel onder eigen verantwoordelijkheid door de aanbieder worden uitgevoerd, met als enige uitzondering AI-systemen die bedoeld zijn om voor biometrie te worden gebruikt.

- (126) Met het oog op de uitvoering van conformiteitsbeoordelingen door derden, wanneer deze vereist zijn, moeten de nationale bevoegde autoriteiten aangemelde instanties aanmelden op grond van deze verordening, mits deze instanties voldoen aan een reeks voorschriften, met name met betrekking tot de onafhankelijkheid, competenties, afwezigheid van belangenconflicten en passende voorschriften inzake cyberbeveiliging. De aanmelding van die instanties moet door de nationale bevoegde autoriteiten aan de Commissie en de andere lidstaten worden gezonden via het op grond van artikel R23 van bijlage I bij Besluit 768/2008/EG door de Commissie ontwikkelde en beheerde elektronische aanmeldingssysteem.
- (127) Het is in overeenstemming met de verbintenissen van de Unie in het kader van de WTO-overeenkomst inzake technische handelsbelemmeringen, passend om de wederzijdse erkenning van door bevoegde conformiteitsbeoordelingsinstanties voortgebrachte conformiteitsbeoordelingsresultaten te bevorderen, ongeacht het grondgebied waar deze instanties zijn gevestigd, met dien verstande dat die naar het recht van een derde land opgerichte instanties voldoen aan de toepasselijke eisen van deze verordening en de Unie daartoe een overeenkomst heeft gesloten. In dit verband moet de Commissie actief op zoek gaan naar mogelijke internationale instrumenten daartoe en zich met name inzetten voor de sluiting van overeenkomsten inzake wederzijdse erkenning met derde landen.

- (128) In lijn met het algemeen erkende begrip van substantiële wijziging van producten die vallen onder de harmonisatiewetgeving van de Unie, is het passend dat, indien zich een verandering voordoet die gevolgen kan hebben voor de overeenstemming van een AI-systeem met een hoog risico met deze verordening (bijvoorbeeld een verandering van het besturingssysteem of de softwarearchitectuur) of indien het beoogde doel van het systeem verandert, dat AI-systeem wordt beschouwd als een nieuw AI-systeem dat aan een nieuwe conformiteitsbeoordeling moet worden onderworpen. Wijzigingen met betrekking tot het algoritme en de prestaties van AI-systemen die blijven “leren” nadat zij in de handel zijn gebracht of in gebruik gesteld, die met name automatisch aanpassen hoe taken worden uitgevoerd, mogen echter geen substantiële wijziging vormen, mits die wijzigingen vooraf door de aanbieder zijn bepaald en op het moment van de conformiteitsbeoordeling zijn beoordeeld.
- (129) Op AI-systemen met een hoog risico moet de CE-markering worden aangebracht om aan te geven dat zij in overeenstemming zijn met deze verordening, zodat het vrije verkeer ervan op de interne markt mogelijk is. Op AI-systemen met een hoog risico die in een product zijn geïntegreerd moet een fysieke CE-markering worden aangebracht, die kan worden aangevuld met een digitale CE-markering. Voor AI-systemen met een hoog risico die alleen digitaal worden verstrekt, moet een digitale CE-markering worden gebruikt. De lidstaten mogen het in de handel brengen en het in gebruik stellen van AI-systemen met een hoog risico die aan de in deze verordening vastgelegde eisen voldoen en waarop de CE-markering is aangebracht, niet op ongerechtvaardigde wijze belemmeren.

- (130) In bepaalde omstandigheden kan de snelle beschikbaarheid van innovatieve technologieën cruciaal zijn voor de gezondheid en veiligheid van personen, de bescherming van het milieu en de klimaatverandering, en de samenleving in haar geheel. Het is derhalve passend dat de markttoezichtautoriteiten om uitzonderlijke redenen in verband met de openbare veiligheid of de bescherming van het leven en de gezondheid van natuurlijke personen, de bescherming van het milieu en de bescherming van essentiële industriële en infrastructurele activa toestemming kunnen verlenen voor het in de handel brengen of in gebruik stellen van AI-systemen die nog niet aan een conformiteitsbeoordeling zijn onderworpen. In naar behoren gemotiveerde situaties, zoals voorzien in deze verordening, kunnen rechtshandavingsinstanties of civielebeschermingsautoriteiten zonder toestemming van de markttoezichtautoriteit een specifiek AI-systeem met een hoog risico in gebruik stellen, op voorwaarde dat tijdens of na het gebruik onverwijld om een dergelijke toestemming wordt verzocht.
- (131) Om de werkzaamheden van de Commissie en de lidstaten op het gebied van AI te vergemakkelijken en om de transparantie voor het publiek te vergroten, moeten aanbieders van AI-systemen met een hoog risico die geen verband houden met producten die onder het toepassingsgebied van de desbetreffende bestaande harmonisatiewetgeving van de Unie vallen, evenals aanbieders die van mening zijn dat een in de in een bijlage bij deze verordening opgenomen gebruiksgevallen met een hoog risico vermeld AI-systeem op basis van een afwijking geen hoog risico inhoudt, worden verplicht zichzelf en informatie over hun AI-systeem te registreren in een EU-databank, die door de Commissie moet worden opgericht en beheerd. Alvorens een in de in een bijlage bij deze verordening opgenomen gebruiksgevallen met een hoog risico vermeld AI-systeem te gebruiken, moeten gebruiksverantwoordelijken van AI-systemen met een hoog risico die overheidsinstanties, -agentschappen of -organen zijn, zich bij een dergelijke databank registreren en het systeem selecteren dat zij voornemens zijn te gebruiken.

Andere gebruiksverantwoordelijken moeten het recht hebben dit vrijwillig te doen. Dit deel van de EU-databank moet voor het publiek toegankelijk en kosteloos zijn, en de informatie moet gemakkelijk te doorzoeken, begrijpelijk en machineleesbaar zijn. De EU-databank moet ook gebruiksvriendelijk zijn, bijvoorbeeld door zoekfuncties aan te bieden, onder meer door middel van trefwoorden, zodat het grote publiek relevante informatie kan vinden die moet worden ingediend bij de registratie van AI-systemen met een hoog risico, evenals informatie over de gebruikssituatie van AI-systemen met een hoog risico, zoals uiteengezet in een bijlage bij deze verordening, waarmee de AI-systemen met een hoog risico overeenstemmen. Ook alle substantiële wijzigingen van AI-systemen met een hoog risico moeten in de EU-databank worden geregistreerd. Voor AI-systemen met een hoog risico op het gebied van rechtshandhaving, migratie, asiel en grenstoezichtsbeheer moeten de registratieverplichtingen worden verricht in een beveiligd niet-openbaar deel van de EU-databank. De toegang tot het beveiligde niet-openbare deel moet strikt worden beperkt tot de Commissie en, wat hun nationale deel van die databank betreft, tot markttoezichtautoriteiten. AI-systemen met een hoog risico op het gebied van kritieke infrastructuur mogen alleen op nationaal niveau worden geregistreerd. De Commissie moet de verwerkingsverantwoordelijke van de EU-databank zijn, overeenkomstig Verordening (EU) 2018/1725. Teneinde de volledige functionaliteit van de EU-databank te waarborgen, moet de procedure voor het vaststellen van de databank de uitwerking van functionele specificaties door de Commissie en een onafhankelijk auditverslag omvatten. De Commissie moet bij de uitvoering van haar taken als verwerkingsverantwoordelijke voor de EU-databank rekening houden met cyberbeveiligingsrisico's. Om de beschikbaarheid en het gebruik van de EU-databank door het publiek te maximaliseren, moet de databank, met inbegrip van de via de EU-databank beschikbaar gestelde informatie, voldoen aan de eisen van Richtlijn (EU) 2019/882.

- (132) Bepaalde AI-systemen die bedoeld zijn om met natuurlijke personen te interageren of om content te genereren, kunnen specifieke risico's op imitatie of misleiding met zich meebrengen, ongeacht of zij als systeem met een hoog risico gelden. In bepaalde omstandigheden moeten voor het gebruik van deze systemen daarom specifieke transparantieplichtingen gelden, zonder dat afbreuk wordt gedaan aan de eisen en verplichtingen voor AI-systemen met een hoog risico, en moeten zij onderworpen zijn aan gerichte uitzonderingen om rekening te houden met de bijzondere behoeften van rechtshandhaving. Met name moeten natuurlijke personen ervan in kennis worden gesteld dat zij interageren met een AI-systeem, tenzij dit duidelijk is vanuit het oogpunt van een normaal geïnformeerde en redelijk opmerkzame en omzichtige natuurlijke persoon, rekening houdend met de omstandigheden en de gebruikscontext. Bij de toepassing van die verplichting moet rekening worden gehouden met de kenmerken van tot kwetsbare groepen horende natuurlijke personen die vanwege hun leeftijd of handicap kwetsbaar zijn, voor zover het AI-systeem bedoeld is om ook met die groepen te interageren. Bovendien moeten natuurlijke personen indien zij worden blootgesteld aan AI-systemen die, door hun biometrische gegevens te verwerken, de emoties of intenties van deze personen kunnen vaststellen of afleiden of hen in een specifieke categorie kunnen indelen, hiervan in kennis worden gesteld. Zulke specifieke categorieën kunnen betrekking hebben op aspecten zoals geslacht, leeftijd, haarkleur, oogkleur, tatoeages, persoonlijke kenmerken, etnische afkomst, persoonlijke voorkeuren en interesses. Dergelijke informatie en kennisgevingen moeten worden verstrekt in een formaat dat toegankelijk is voor personen met een handicap.

- (133) Bepaalde AI-systemen kunnen grote hoeveelheden synthetische content genereren waarbij het voor de mens steeds moeilijker wordt deze te onderscheiden van door de mens gegenereerde en authentieke content. De brede beschikbaarheid en de toenemende capaciteit van deze systemen hebben een aanzienlijke impact op de integriteit van en het vertrouwen in het informatie-ecosysteem, waardoor nieuwe risico's op desinformatie en manipulatie op grote schaal, fraude, imitatie en consumentenbedrog ontstaan. In het licht van die effecten, het snelle technologische tempo en de behoefte aan nieuwe methoden en technieken om de oorsprong van informatie te traceren, is het passend aanbieders van die systemen voor te schrijven dat zij technische oplossingen inbouwen die markering in een machineleesbaar formaat mogelijk maken en aantonen dat de output is gegenereerd of gemanipuleerd door een AI-systeem en niet door een mens. Dergelijke technieken en methoden moeten voldoende betrouwbaar, interoperabel, doeltreffend en robuust zijn, voor zover dit technisch haalbaar is, rekening houdend met de beschikbare technieken of een combinatie van dergelijke technieken, zoals watermerken, metagegevens, cryptografische methoden voor het aantonen van de herkomst en authenticiteit van inhoud, loggingmethoden, vingerafdrukken of andere technieken, naargelang het geval. Bij de uitvoering van deze verplichting moeten aanbieders ook rekening houden met de specifieke kenmerken en beperkingen van de verschillende soorten content en de relevante technologische en marktontwikkelingen op dit gebied, zoals blijkt uit de algemeen erkende stand van de techniek. Dergelijke technieken en methoden kunnen worden toegepast op het niveau van het AI-systeem of op het niveau van het AI-model, met inbegrip van AI-modellen voor algemene doeleinden die content genereren, waardoor de aanbieder verder in de AI-waardeketen van het AI-systeem gemakkelijker aan deze verplichting kan voldoen. Met het oog op de evenredigheid, moet worden overwogen dat deze markeringsverplichting niet van toepassing mag zijn op AI-systemen die in de eerste plaats een ondersteunende functie hebben voor het uitvoeren van standaardbewerkingen of op AI-systemen die de door de gebruiksverantwoordelijke verstrekte inputdata, of de semantiek ervan, niet wezenlijk wijzigen.

- (134) Naast de technische oplossingen die door de aanbieders van het AI-systeem worden gebruikt, moeten gebruiksverantwoordelijken die een AI-systeem gebruiken om beeld-, audio- of video-content te genereren of te manipuleren die aanzienlijk lijkt op bestaande personen, voorwerpen, plaatsen, entiteiten of gebeurtenissen en voor een persoon ten onrechte authentiek of waarachtig kunnen lijken (deepfakes), ook klaar en duidelijk kenbaar maken dat de content kunstmatig is gecreëerd of gemanipuleerd door de AI-output als zodanig aan te merken en de kunstmatige oorsprong ervan bekend te maken. Naleving van deze transparantieverplichting mag niet aldus worden uitgelegd dat het gebruik van het AI-systeem of de output ervan afbreuk doet aan het in het Handvest gewaarborgde recht op vrijheid van meningsuiting en het recht op vrijheid van kunsten en wetenschappen belemmert, met name indien de content deel uitmaakt van een werk of programma dat duidelijk creatief, satirisch, artistiek, fictief of analoog van aard is, met inachtneming van passende waarborgen voor de rechten en vrijheden van derden. In die gevallen is de in deze verordening vastgestelde transparantieverplichting voor deepfakes beperkt tot de openbaarmaking van het bestaan van dergelijke gegenereerde of gemanipuleerde content, en dit op een passende wijze die geen belemmering vormt voor de weergave of het genot van het werk, met inbegrip van de normale exploitatie en het normale gebruik ervan, met behoud van het nut en de kwaliteit van het werk. Daarnaast is het ook passend te voorzien in een soortgelijke openbaarmakingsplicht met betrekking tot door AI gegenereerde of gemanipuleerde tekst, voor zover deze wordt gepubliceerd met als doel het publiek te informeren over aangelegenheden van algemeen belang, tenzij de door AI gegenereerde content een proces van menselijke toetsing of redactionele controle heeft ondergaan en een natuurlijke of rechtspersoon redactionele verantwoordelijkheid draagt voor de publicatie van de content.

- (135) Onverminderd het verplichte karakter en de volledige toepasselijkheid van de transparantieverplichtingen, kan de Commissie ook het opstellen van praktijkcodes op het niveau van de Unie aanmoedigen en faciliteren om de doeltreffende uitvoering van de verplichtingen met betrekking tot het opsporen en het aanmerken van kunstmatig gegenereerde of gemanipuleerde content te vergemakkelijken, onder meer ter ondersteuning van praktische regelingen voor, in voorkomend geval, het toegankelijk maken van de detectiemechanismen en het faciliteren van samenwerking met andere actoren in de waardeketen, het verspreiden van content of het controleren van de authenticiteit en herkomst ervan, teneinde het publiek in staat te stellen door AI gegenereerde content doeltreffend te onderscheiden.
- (136) De verplichtingen die in deze verordening aan aanbieders en gebruiksverantwoordelijken van bepaalde AI-systemen worden opgelegd om opsporing mogelijk te maken, evenals de bekendmaking dat de outputs van die systemen kunstmatig worden gegenereerd of gemanipuleerd, zijn bijzonder relevant om de doeltreffende uitvoering van Verordening (EU) 2022/2065 te vergemakkelijken. Dit geldt met name voor de verplichtingen van aanbieders van zeer grote onlineplatforms of zeer grote onlinezoekmachines om systeemrisico's te identificeren en te beperken die kunnen voortvloeien uit de verspreiding van kunstmatig gegenereerde of gemanipuleerde content, met name het risico op feitelijke of voorzienbare negatieve effecten op democratische processen, het maatschappelijk debat en verkiezingsprocessen, onder meer door desinformatie. Het vereiste om uit hoofde van deze verordening content die door AI-systemen wordt gegenereerd, aan te merken, doet geen afbreuk aan de verplichting van artikel 16, lid 6, van Verordening (EU) 2022/2065 voor aanbieders van hostingdiensten om meldingen van illegale content te verwerken op grond van artikel 16, lid 1, van die verordening, en mag geen invloed hebben op de beoordeling van en het besluit over de onwettigheid van de specifieke content. Die beoordeling moet uitsluitend worden verricht aan de hand van de regels inzake de rechtmatigheid van de content.

- (137) Naleving van de bovengenoemde transparantieplichtingen voor AI-systemen die onder deze verordening vallen, mag niet aldus worden uitgelegd dat het gebruik van het systeem of de output ervan rechtmatig is op grond van deze verordening of andere wetgeving van de Unie en de lidstaten, en moet andere in het Unierecht of het nationale recht vastgelegde transparantieplichtingen voor gebruiksverantwoordelijken van AI-systemen onverlet laten.
- (138) AI is een snel ontwikkelende familie van technologieën die regelgevingstoezicht en een veilige en gecontroleerde plek voor experimenteren vereist, terwijl tegelijkertijd de verantwoorde innovatie en integratie van passende waarborgen en risicobeperkende maatregelen worden gewaarborgd. Om te zorgen voor een wettelijk kader dat innovatie stimuleert, toekomstbestendig is en bestand is tegen verstoringen, moeten de lidstaten ervoor zorgen dat hun nationale bevoegde autoriteiten ten minste één AI-testomgeving voor regelgeving op nationaal niveau tot stand brengen om de ontwikkeling en het testen van innovatieve AI-systemen onder strikt regelgevingstoezicht mogelijk te maken voordat deze systemen in de handel worden gebracht of anderszins in gebruik worden gesteld. De lidstaten kunnen deze verplichting ook nakomen door deel te nemen aan reeds bestaande testomgevingen voor regelgeving of door samen met de bevoegde autoriteiten van een of meer lidstaten een testomgeving op te zetten, voor zover deze deelname de deelnemende lidstaten een gelijkwaardig niveau van nationale dekking biedt. AI-testomgevingen voor regelgeving kunnen in fysieke, digitale of hybride vorm worden opgezet en kunnen zowel fysieke als digitale producten bevatten. De autoriteiten die de AI-testomgeving hebben ontwikkeld, moeten er ook voor zorgen dat de AI-testomgevingen voor regelgeving over voldoende middelen beschikken, met inbegrip van financiële en personele middelen.

- (139) De doelstellingen van AI-testomgevingen voor regelgeving moeten bestaan in het bevorderen van AI-innovatie door te zorgen voor een gecontroleerde experiment- en testomgeving in de ontwikkelingsfase en de fase vóór het in de handel brengen met het oog op het waarborgen van de overeenstemming van innovatieve AI-systemen met deze verordening en andere relevante wetgeving van de Unie en de lidstaten. Bovendien moeten de AI-testomgevingen voor regelgeving gericht zijn op het verbeteren van de rechtszekerheid voor innovatoren en het toezicht en begrip van de bevoegde autoriteiten ten aanzien van de mogelijkheden, opkomende risico's en de effecten van het gebruik van AI, het leren van regelgeving voor autoriteiten en ondernemingen te vergemakkelijken, onder meer met het oog op toekomstige aanpassingen van het rechtskader, de samenwerking en de uitwisseling van beste praktijken met de autoriteiten die betrokken zijn bij de AI-testomgeving voor regelgeving te ondersteunen, en het versnellen van de toegang tot markten, onder meer door belemmeringen voor kmo's, met inbegrip van start-ups, weg te nemen. AI-testomgevingen voor regelgeving moeten in de hele Unie op grote schaal beschikbaar zijn, en er moet bijzondere aandacht worden besteed aan de toegankelijkheid ervan voor kmo's, met inbegrip van start-ups. Bij deelname aan een AI-testomgeving voor regelgeving moet de focus liggen op kwesties die leiden tot rechtsonzekerheid voor aanbieders en potentiële aanbieders met betrekking tot innovatie, experimenten met AI in de Unie en bijdragen aan het empirisch leren op het gebied van regelgeving. Toezicht op de AI-systemen in een AI-testomgeving voor regelgeving moet daarom gericht zijn op het ontwikkelen, trainen, testen en valideren van deze systemen, voordat ze in de handel worden gebracht of in gebruik worden gesteld, alsook op het begrip substantiële wijziging en het zich voordoen ervan, hetgeen een nieuwe conformiteitsbeoordelingsprocedure kan vereisen. Aanzienlijke risico's die tijdens het ontwikkelen en testen van dergelijke AI-systemen worden vastgesteld, moeten op adequate wijze worden beperkt en bij gebreke daarvan leiden tot de opschorting van het ontwikkelings- en testproces.

Waar passend moeten nationale bevoegde autoriteiten die AI-testomgevingen voor regelgeving opzetten, samenwerken met andere betrokken autoriteiten, waaronder autoriteiten die toezicht houden op de bescherming van de grondrechten, en kunnen zij toestaan dat andere actoren binnen het AI-ecosysteem hierbij betrokken worden, zoals nationale of Europese normalisatie-instellingen, aangemelde instanties, test- en experimenteerfaciliteiten, laboratoria voor onderzoek en experimenteren, Europese digitale-innovatiehubs en relevante belanghebbenden en maatschappelijke organisaties. Teneinde de uniforme uitvoering in de gehele Unie en schaalvoordelen te waarborgen, is het passend om gemeenschappelijke regels vast te stellen voor de uitvoering van AI-testomgevingen voor regelgeving, evenals een kader voor de samenwerking tussen de relevante autoriteiten die betrokken zijn bij het toezicht op de testomgevingen. Krachtens deze verordening opgezette AI-testomgevingen voor regelgeving mogen geen afbreuk doen aan andere wetgeving op grond waarvan andere testomgevingen kunnen worden opgezet om de naleving van ander recht dan deze verordening te waarborgen. Waar passend moeten de bevoegde autoriteiten die verantwoordelijk zijn voor die andere testomgevingen voor regelgeving nagaan welke voordelen het zou opleveren als die testomgevingen ook worden gebruikt om te waarborgen dat AI-systemen in overeenstemming zijn met deze verordening. Als de nationale bevoegde autoriteiten en de deelnemers aan de AI-testomgeving voor regelgeving het hierover eens zijn, kunnen in het kader van de AI-testomgeving voor regelgeving ook testen onder reële omstandigheden worden uitgevoerd en gecontroleerd.

- (140) Deze verordening moet aanbieders en potentiële aanbieders van de AI-testomgeving voor regelgeving de rechtsgrond bieden voor het gebruik van persoonsgegevens die voor andere doeleinden zijn verzameld, met het oog op de ontwikkeling van bepaalde AI-systemen in het openbaar belang in de AI-testomgeving voor regelgeving, echter alleen onder bepaalde omstandigheden, overeenkomstig artikel 6, lid 4, en artikel 9, lid 2, punt g), van Verordening (EU) 2016/679 en de artikelen 5, 6 en 10 van Verordening (EU) 2018/1725 en onverminderd artikel 4, lid 2, en artikel 10 van Richtlijn (EU) 2016/680. Alle andere verplichtingen van verwerkingsverantwoordelijken en rechten van betrokkenen uit hoofde van Verordening (EU) 2016/679, Verordening (EU) 2018/1725 en Richtlijn (EU) 2016/680 blijven van toepassing. In het bijzonder mag deze verordening geen rechtsgrond bieden in de zin van artikel 22, lid 2, punt b), van Verordening (EU) 2016/679 en artikel 24, lid 2, punt b), van Verordening (EU) 2018/1725. Aanbieders en potentiële aanbieders van de AI-testomgeving voor regelgeving moeten zorgen voor passende waarborgen en moeten samenwerken met de bevoegde autoriteiten, onder meer door hun richtsnoeren te volgen en snel en te goeder trouw te handelen om eventuele vastgestelde significante risico's voor de veiligheid, de gezondheid en de grondrechten die zich tijdens de ontwikkeling en het experimenteren in die testomgeving kunnen voordoen, op adequate wijze te beperken.

- (141) Om de ontwikkeling en het in de handel brengen van de in een bijlage bij deze verordening opgenomen AI-systemen met een hoog risico te versnellen is het belangrijk dat aanbieders of potentiële aanbieders van deze systemen ook zonder deel te nemen aan een AI-testomgeving voor regelgeving gebruik kunnen maken van een speciale regeling voor het testen van deze systemen onder reële omstandigheden. De verordening moet in dergelijke gevallen echter voorzien in passende en voldoende waarborgen en voorwaarden voor aanbieders en potentiële aanbieders, rekening houdend met de mogelijke gevolgen van die testen voor individuele natuurlijke personen. Deze waarborgen moeten onder meer inhouden dat natuurlijke personen om geïnformeerde toestemming wordt gevraagd voor deelname aan testen onder reële omstandigheden, behalve in het kader van rechtshandhaving waarbij het vragen van geïnformeerde toestemming zou verhinderen dat het AI-systeem wordt getest. Toestemming van proefpersonen voor deelname aan dergelijke tests in het kader van deze verordening staat los van de toestemming van betrokkenen voor de verwerking van hun persoonsgegevens uit hoofde van het relevante gegevensbeschermingsrecht en laat deze onverlet.

Het is ook belangrijk om de risico's tot een minimum te beperken en toezicht door bevoegde autoriteiten mogelijk te maken en daarom potentiële aanbieders voor te schrijven dat zij een plan voor testen onder reële omstandigheden indienen bij de bevoegde markttoezichtautoriteit, de testen registreren in specifieke rubrieken in de EU-databank, met uitzondering van enkele beperkte uitzonderingen, beperkingen stellen aan de periode gedurende welke de testen kunnen worden uitgevoerd en aanvullende waarborgen voor tot bepaalde kwetsbare groepen horende personen vereisen, evenals een schriftelijke overeenkomst waarin de rollen en verantwoordelijkheden van potentiële aanbieders en gebruiksverantwoordelijken worden omschreven en doeltreffend toezicht door bevoegd personeel dat betrokken is bij de testen onder reële omstandigheden. Voorts is het passend te voorzien in aanvullende waarborgen om ervoor te zorgen dat de voorspellingen, aanbevelingen of besluiten van het AI-systeem daadwerkelijk kunnen worden teruggedraaid en genegeerd en dat persoonsgegevens worden beschermd en gewist indien de proefpersonen hun toestemming om aan de testen deel te nemen hebben ingetrokken, onverminderd hun rechten als betrokkenen uit hoofde van het Unierecht inzake gegevensbescherming. Wat de doorgifte van gegevens betreft, is het ook passend te voorzien dat gegevens die zijn verzameld en verwerkt met het oog op testen in reële omstandigheden alleen aan derde landen mogen worden doorgegeven die passende en toepasselijke waarborgen uit hoofde van het Unierecht toepassen, met name in overeenstemming met de basisvoorwaarden voor de doorgifte van persoonsgegevens uit hoofde van het Unierecht inzake gegevensbescherming, terwijl voor niet-persoonsgebonden gegevens passende waarborgen worden voorzien in overeenstemming met het Unierecht, zoals Verordeningen (EU) 2022/868⁴² en (EU) 2023/2854⁴³ van het Europees Parlement en de Raad.

⁴² Verordening (EU) 2022/868 van het Europees Parlement en de Raad van 30 mei 2022 betreffende Europese datagovernance en tot wijziging van Verordening (EU) 2018/1724 (Datagovernanceverordening) (PB L 152 van 3.6.2022, blz. 1).

⁴³ Verordening (EU) 2023/2854 van het Europees Parlement en de Raad van 13 december 2023 betreffende geharmoniseerde regels inzake eerlijke toegang tot en eerlijk gebruik van data en tot wijziging van Verordening (EU) 2017/2394 en Richtlijn (EU) 2020/1828 (Dataverordening) (PB L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

- (142) Om ervoor te zorgen dat AI tot sociaal en ecologisch gunstige resultaten leidt, worden de lidstaten aangemoedigd onderzoek naar en ontwikkeling van AI-oplossingen ter ondersteuning van sociaal en ecologisch gunstige resultaten te steunen en te bevorderen, zoals op AI gebaseerde oplossingen om de toegankelijkheid voor personen met een handicap te vergroten, sociaal-economische ongelijkheden aan te pakken of milieudoelstellingen te halen, door voldoende middelen toe te wijzen, met inbegrip van overheidsfinanciering en financiering door de Unie, en met name, in voorkomend geval en op voorwaarde dat aan de subsidiabiliteits- en selectiecriteria is voldaan, vooral projecten in overweging te nemen waarmee dergelijke doelstellingen worden nagestreefd. Dergelijke projecten moeten gebaseerd zijn op het beginsel van interdisciplinaire samenwerking tussen AI-ontwikkelaars, deskundigen op het gebied van ongelijkheid en non-discriminatie, toegankelijkheid, consumentenrecht, milieurecht en digitale rechten, alsook academici.

- (143) Om de innovatie te bevorderen en beschermen, is het belangrijk dat er in het bijzonder rekening wordt gehouden met de belangen van kmo's, met inbegrip van start-ups, die aanbieders of gebruiksverantwoordelijken van AI-systemen zijn. Daartoe moeten de lidstaten initiatieven ontwikkelen die gericht zijn op deze operatoren, onder meer met het oog op bewustmaking en informatieverstrekking. De lidstaten moeten kmo's, met inbegrip van start-ups, die een maatschappelijke zetel of een bijkantoor in de Unie hebben, prioritaire toegang bieden tot de AI-testomgevingen voor regelgeving, mits zij voldoen aan de subsidiabiliteits-voorwaarden en selectiecriteria en zonder andere aanbieders en potentiële aanbieders uit te sluiten van de testomgevingen, mits aan dezelfde voorwaarden en criteria is voldaan. De lidstaten moeten hiervoor de bestaande kanalen gebruiken en waar nodig nieuwe specifieke kanalen voor de communicatie met kmo's, met inbegrip van start-ups, gebruiksverantwoordelijken, andere innovatoren en, in voorkomend geval, lokale overheidsinstanties opzetten om kmo's in hun ontwikkelingstraject te ondersteunen door begeleiding te bieden en vragen over de uitvoering van deze verordening te beantwoorden. Waar nodig moeten deze kanalen met elkaar samenwerken om synergieën te creëren en te zorgen voor een homogene aanpak bij hun adviezen aan kmo's, met inbegrip van start-ups, en gebruiksverantwoordelijken. Daarnaast moeten de lidstaten de deelname van kmo's en andere relevante belanghebbenden aan het proces voor de ontwikkeling van normen faciliteren. Bovendien moet rekening worden gehouden met de specifieke belangen en behoeften van aanbieders die kmo's zijn, met inbegrip van start-ups, wanneer aangemelde instanties bijdragen voor de conformiteitsbeoordeling vaststellen. De Commissie moet de certificerings- en nalevingskosten voor kmo's, met inbegrip van start-ups, regelmatig beoordelen via transparant overleg, en moet met de lidstaten samenwerken om die kosten te verlagen.

Vertaalkosten in verband met verplichte documentatie en communicatie met autoriteiten kunnen bijvoorbeeld een aanzienlijke kostenpost vormen voor met name kleine aanbieders en andere operatoren. De lidstaten moeten er indien mogelijk voor zorgen dat een van de door hen vastgestelde en aanvaarde talen voor de documentatie van betrokken aanbieders en voor de communicatie met operatoren in grote lijnen wordt begrepen door een zo groot mogelijk aantal grensoverschrijdende gebruiksverantwoordelijken. Om tegemoet te komen aan de specifieke behoeften van kmo's, met inbegrip van start-ups, moet de Commissie op verzoek van de AI-board gestandaardiseerde sjablonen verstrekken voor de gebieden die onder deze verordening vallen. Daarnaast moet de Commissie de inspanningen van de lidstaten aanvullen door te voorzien in een centraal informatieplatform met gebruiksvriendelijke informatie over deze verordening voor alle aanbieders en gebruiksverantwoordelijken, door passende communicatiecampagnes te organiseren om het bewustzijn over de uit deze verordening voortvloeiende verplichtingen te vergroten, en door de convergentie van beste praktijken in openbare aanbestedingsprocedures met betrekking tot AI-systemen te evalueren en te bevorderen. Middelgrote ondernemingen die tot voor kort als kleine ondernemingen werden aangemerkt in de zin van de bijlage bij Aanbeveling 2003/361/EG van de Commissie⁴⁴, moeten toegang hebben tot die steunmaatregelen, aangezien die nieuwe middelgrote ondernemingen soms niet over de nodige juridische middelen en opleiding beschikken om een goed begrip en een goede naleving van deze verordening te waarborgen.

⁴⁴ Aanbeveling van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (PB L 124 van 20.5.2003, blz. 36).

- (144) Om innovatie te bevorderen en te beschermen moeten het platform voor AI on demand en alle relevante financieringsprogramma's en projecten van de Unie, zoals het programma Digitaal Europa en Horizon Europa, die op Unie- of nationaal niveau worden uitgevoerd door de Commissie en de lidstaten, in voorkomend geval, bijdragen aan de verwezenlijking van de doelstellingen van deze verordening.
- (145) Om de risico's voor de uitvoering te beperken die voortvloeien uit een gebrek aan kennis en deskundigheid op de markt en om de nakoming door aanbieders, met name kmo's, met inbegrip van start-ups, en aangemelde instanties van hun verplichtingen uit hoofde van deze verordening te vergemakkelijken, zouden met name het platform voor AI on demand, de Europese digitale-innovatiehubs en de test- en experimenteerfaciliteiten die door de Commissie en de lidstaten op Unie- of nationaal niveau zijn vastgesteld, moeten bijdragen tot de uitvoering van deze verordening. Binnen hun respectieve opdracht en bevoegdheidsgebieden kunnen het platform voor AI on demand, de Europese digitale-innovatiehubs en de test- en experimenteerfaciliteiten met name technische en wetenschappelijke ondersteuning bieden aan aanbieders en aangemelde instanties.

- (146) Voorts is het, gezien de zeer kleine omvang van sommige operatoren en om de evenredigheid met betrekking tot de kosten van innovatie te waarborgen, passend dat micro-ondernemingen op vereenvoudigde wijze aan een van de duurste vereisten, namelijk het opzetten van een systeem voor kwaliteitsbeheer, voldoen, hetgeen de administratieve lasten en de kosten voor deze ondernemingen zou verminderen zonder afbreuk te doen aan het beschermingsniveau en de noodzaak om de vereisten voor AI-systemen met een hoog risico na te leven. De Commissie moet richtsnoeren ontwikkelen om de elementen te specificeren van het kwaliteitsbeheersysteem waaraan micro-ondernemingen op deze vereenvoudigde wijze moeten voldoen.
- (147) Het is passend dat de Commissie voor zover mogelijk de toegang tot test- en experimenteerfaciliteiten vergemakkelijkt voor instanties, groepen of laboratoria die overeenkomstig relevante harmonisatiewetgeving van de Unie zijn opgericht of erkend en die taken uitvoeren in het kader van de conformiteitsbeoordeling van producten of apparaten die onder die harmonisatiewetgeving van de Unie vallen. Dit is met name het geval voor deskundigenpanels, deskundige laboratoria en referentielaboratoria op het gebied van medische hulpmiddelen overeenkomstig de Verordeningen (EU) 2017/745 en (EU) 2017/746.

(148) Bij deze verordening moet een governancekader worden vastgelegd dat het mogelijk maakt de toepassing van deze verordening op nationaal niveau te coördineren en te ondersteunen, evenals capaciteiten op het niveau van de Unie op te bouwen en belanghebbenden op het gebied van AI te integreren. De doeltreffende uitvoering en handhaving van deze verordening vereist een governancekader dat het mogelijk maakt centrale deskundigheid op het niveau van de Unie te coördineren en uit te bouwen. Het AI-bureau is opgericht bij besluit van de Commissie⁴⁵ en heeft tot taak deskundigheid en capaciteiten van de Unie op het gebied van AI te ontwikkelen en bij te dragen aan de uitvoering van het recht van de Unie inzake AI. De lidstaten moeten de taken van het AI-bureau faciliteren om de ontwikkeling van deskundigheid en capaciteiten van de Unie op het niveau van de Unie te ondersteunen en de werking van de digitale eengemaakte markt te versterken. Voorts moeten een raad, bestaande uit vertegenwoordigers van de lidstaten, een wetenschappelijk panel om de wetenschappelijke gemeenschap te integreren en een adviesforum worden opgericht om te zorgen voor inbreng van belanghebbenden bij de uitvoering van deze verordening op Unie- en nationaal niveau. Bij de ontwikkeling van de deskundigheid en capaciteiten van de Unie moet ook gebruik worden gemaakt van bestaande middelen en deskundigheid, met name door middel van synergieën met structuren die zijn opgebouwd in het kader van de handhaving van andere wetgeving op Unieniveau en synergieën met gerelateerde initiatieven op Unieniveau, zoals de Gemeenschappelijke onderneming EuroHPC en de test- en experimenteerfaciliteiten voor AI in het kader van het programma Digitaal Europa.

⁴⁵ Besluit van de Commissie van 24.1.2024 tot oprichting van het Europees Bureau voor artificiële intelligentie (C/2024/390).

- (149) Teneinde een soepele, doeltreffende en geharmoniseerde uitvoering van deze verordening mogelijk te maken, moet een AI-board worden opgericht. De AI-board moet de verschillende belangen van het AI-ecosysteem belichamen en uit vertegenwoordigers van de lidstaten bestaan. De AI-board moet verantwoordelijk zijn voor een aantal adviestaken, met inbegrip van het opstellen van adviezen en aanbevelingen of het bijdragen aan richtsnoeren over kwesties die verband houden met de uitvoering van deze verordening, waaronder over handhaving, technische specificaties of bestaande normen met betrekking tot de eisen van deze verordening, en de adviesverlening aan de Commissie en de lidstaten en hun nationale bevoegde autoriteiten ten aanzien van specifieke vragen in verband met artificiële intelligentie. Om de lidstaten enige flexibiliteit te bieden bij de aanwijzing van hun vertegenwoordigers in de AI-board, mogen zij iedereen die tot een overheidsinstantie behoort en over relevante competenties en bevoegdheden beschikt om de coördinatie op nationaal niveau te vergemakkelijken en bij te dragen aan de vervulling van de taken van de AI-board aanwijzen als vertegenwoordiger. De AI-board moet twee permanente subgroepen oprichten om een platform te bieden voor samenwerking en uitwisseling tussen markttoezichtautoriteiten en aanmeldende autoriteiten over kwesties betreffende respectievelijk markttoezicht en aangemelde instanties. De permanente subgroep voor markttoezicht moet fungeren als de administratievesamenwerkingsgroep (ADCO) voor deze verordening in de zin van artikel 30 van Verordening (EU) 2019/1020. Overeenkomstig artikel 33 van die verordening moet de Commissie de activiteiten van de permanente subgroep voor markttoezicht ondersteunen door marktevaluaties of -studies uit te voeren, met name om in kaart te brengen voor welke aspecten van deze verordening specifiek en dringend coördinatie nodig is tussen markttoezichtautoriteiten. De AI-board kan in voorkomend geval andere permanente of tijdelijke subgroepen oprichten om specifieke kwesties te onderzoeken. De AI-board moet, in voorkomend geval, ook samenwerken met relevante Unie-organen, -deskundigengroepen en -netwerken die zich bezighouden met het relevante recht van de Unie, waaronder met name die welke actief zijn in het kader van het recht van de Unie inzake data, digitale producten en diensten.

- (150) Om ervoor te zorgen dat belanghebbenden bij de uitvoering en toepassing van deze verordening worden betrokken, moet een adviesforum worden opgericht om de raad en de Commissie advies en technische expertise te verstrekken. Met het oog op een gevarieerde en evenwichtige vertegenwoordiging van belanghebbenden tussen commerciële en niet-commerciële belangen en, binnen de categorie commerciële belangen, wat kmo's en andere ondernemingen betreft, moet het adviesforum onder meer bestaan uit vertegenwoordigers van de industrie, start-ups, kmo's, de academische wereld, het maatschappelijk middenveld, met inbegrip van de sociale partners, het Bureau voor de grondrechten, Enisa, het Europees Comité voor Normalisatie (CEN), het Europees Comité voor elektrotechnische normalisatie (Cenelec) en het Europees Instituut voor telecommunicatienormen (ETSI).
- (151) Ter ondersteuning van de uitvoering en handhaving van deze verordening, met name de monitoringactiviteiten van het AI-bureau met betrekking tot AI-modellen voor algemene doeleinden, moet een wetenschappelijk panel van onafhankelijke deskundigen worden opgericht. De onafhankelijke deskundigen die het wetenschappelijk panel vormen, moeten worden geselecteerd op basis van actuele wetenschappelijke of technische deskundigheid op het gebied van AI en moeten hun taken onpartijdig en objectief uitvoeren en de vertrouwelijkheid van de bij de uitvoering van hun taken en activiteiten verkregen informatie en gegevens waarborgen. Om nationale capaciteit die nodig is voor de doeltreffende handhaving van deze verordening te kunnen versterken, moeten de lidstaten voor hun handhavingsactiviteiten steun kunnen vragen van de deskundigen die het wetenschappelijke panel vormen.

- (152) Om een adequate handhaving van AI-systemen te ondersteunen en de capaciteiten van de lidstaten te versterken, moeten ondersteunende Uniestructuren voor AI-testen worden opgezet en ter beschikking van de lidstaten worden gesteld.
- (153) De lidstaten spelen een belangrijke rol bij de toepassing en handhaving van deze verordening. In dit verband moet elke lidstaat ten minste een anmeldende autoriteit en ten minste een markttoezichtautoriteit als nationale bevoegde autoriteiten aanwijzen voor het toezicht op de toepassing en uitvoering van deze verordening. De lidstaten kunnen besluiten om het even welke soort openbare entiteit aan te wijzen om de taken van de nationale bevoegde autoriteiten in de zin van deze verordening uit te voeren, in overeenstemming met hun specifieke nationale organisatorische kenmerken en behoeften. Om de efficiëntie van de organisatie aan de kant van de lidstaten te verbeteren en een centraal contactpunt in te stellen voor het publiek en andere partijen op het niveau van de lidstaten en de Unie, moet elke lidstaat één markttoezichtautoriteit aanwijzen die als centraal contactpunt moet dienen.
- (154) De nationale bevoegde autoriteiten moeten hun bevoegdheden onafhankelijk, onpartijdig en onbevooroordeeld uitoefenen, teneinde de beginselen van objectiviteit van hun activiteiten en taken te waarborgen en de toepassing en uitvoering van deze verordening te verzekeren. De leden van deze autoriteiten moeten zich onthouden van handelingen die onverenigbaar zijn met hun taken en moeten onderworpen zijn aan vertrouwelijkheidsregels uit hoofde van deze verordening.

- (155) Om ervoor te zorgen dat aanbieders van AI-systemen met een hoog risico rekening kunnen houden met de ervaring met het gebruik van AI-systemen met een hoog risico voor het verbeteren van hun systemen en het ontwerp- en ontwikkelingsproces of tijdig eventuele mogelijke corrigerende maatregelen kunnen nemen, moeten alle aanbieders beschikken over een systeem voor monitoring na het in de handel brengen. In voorkomend geval moet de monitoring na het in de handel brengen een analyse van de interactie met andere AI-systemen, met inbegrip van andere apparaten en software, omvatten. Monitoring na het in de handel brengen mag niet gelden voor gevoelige operationele gegevens van gebruiksverantwoordelijken die rechtshandavingsinstanties zijn. Dit systeem is ook belangrijk om te waarborgen dat de mogelijke risico's van AI-systemen die blijven "leren" nadat zij in de handel zijn gebracht of in gebruik zijn gesteld, op efficiëntere en tijdigere wijze kunnen worden aangepakt. In dit verband moeten aanbieders ook worden verplicht over een systeem te beschikken om ernstige incidenten als gevolg van het gebruik van hun AI-systemen, d.w.z. incidenten of storingen die leiden tot de dood of ernstige schade aan de gezondheid, ernstige en onomkeerbare verstoring van het beheer en de exploitatie van kritieke infrastructuur, inbreuken op verplichtingen uit hoofde van het Unierecht ter bescherming van de grondrechten of ernstige schade aan eigendommen of het milieu, aan de relevante autoriteiten te melden.

(156) Teneinde een passende en doeltreffende handhaving te waarborgen van de eisen en verplichtingen van deze verordening, die valt onder de harmonisatiewetgeving van de Unie, moet het systeem van markttoezicht en de conformiteit van producten, zoals vastgesteld bij Verordening (EU) 2019/1020, volledig van toepassing zijn. Krachtens deze verordening aangewezen markttoezichtautoriteiten moeten over alle handhavingsbevoegdheden beschikken die in deze verordening en in Verordening (EU) 2019/1020 zijn vastgelegd, en moeten hun bevoegdheden en taken onafhankelijk, onpartijdig en onbevooroordeeld uitoefenen. Hoewel voor de meeste AI-systemen geen specifieke eisen en verplichtingen gelden krachtens deze verordening, mogen markttoezichtautoriteiten maatregelen nemen ten aanzien van alle AI-systemen indien deze een risico vormen overeenkomstig deze verordening. Gezien de specifieke aard van de instellingen, agentschappen en organen van de Unie die binnen het toepassingsgebied van deze verordening vallen, is het wenselijk de Europese Toezichthouder voor gegevensbescherming aan te wijzen als de voor hen bevoegde markttoezichtautoriteit. Dit moet de aanwijzing van nationale bevoegde autoriteiten door de lidstaten onverlet laten. Markttoezichtactiviteiten mogen geen afbreuk doen aan het vermogen van de onder toezicht staande entiteiten om hun taken onafhankelijk uit te voeren, indien het Unierecht deze onafhankelijkheid vereist.

- (157) Deze verordening doet geen afbreuk aan de bekwaamheid, taken, bevoegdheden en onafhankelijkheid van betrokken nationale overheidsinstanties of -organen die toezicht houden op de toepassing van het Unierecht voor de bescherming van de grondrechten, met inbegrip van instanties voor gelijke behandeling en gegevensbeschermingsautoriteiten. Waar noodzakelijk met het oog op hun taken, moeten die nationale overheidsinstanties en -organen ook toegang hebben tot eventuele documentatie die op grond van deze verordening wordt opgesteld. Er moet een specifieke vrijwarings-procedure worden vastgesteld om te zorgen voor een adequate en tijdige handhaving ten aanzien van AI-systemen die een risico inhouden voor de gezondheid, veiligheid en de grondrechten. De procedure voor dergelijke AI-systemen die een risico inhouden moet worden toegepast op AI-systemen met een hoog risico die een risico inhouden, verboden systemen die in de handel zijn gebracht, in gebruik zijn gesteld of zijn gebruikt in strijd met de bepalingen van deze verordening inzake verboden praktijken en AI-systemen die beschikbaar zijn gemaakt in strijd met de transparantievereisten van deze verordening en een risico inhouden.

- (158) Het Unierecht inzake financiële diensten omvat regels en eisen met betrekking tot interne governance en risicobeheer die van toepassing zijn op gereguleerde financiële instellingen bij het verlenen van deze diensten, ook indien zij gebruikmaken van AI-systemen. Om te zorgen voor een coherente toepassing en handhaving van de verplichtingen uit hoofde van deze verordening en de relevante regels en vereisten van de rechtshandelingen van de Unie inzake financiële diensten, moeten de bevoegde autoriteiten voor het toezicht op en de handhaving van die rechtshandelingen, met name bevoegde autoriteiten zoals gedefinieerd in Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad⁴⁶ en de Richtlijnen 2008/48/EG⁴⁷, 2009/138/EG⁴⁸, 2013/36/EU⁴⁹, 2014/17/EU⁵⁰ en (EU) 2016/97⁵¹ van het Europees Parlement en de Raad, binnen hun respectieve bevoegdheden worden aangewezen als bevoegde autoriteiten voor het toezicht op de uitvoering van deze verordening, met inbegrip van markttoezichtactiviteiten, met betrekking tot AI-systemen die worden aangeboden of gebruikt door gereguleerde en gecontroleerde financiële instellingen, tenzij de lidstaten besluiten een andere autoriteit aan te wijzen om deze markttoezichttaken uit te voeren.

⁴⁶ Verordening (EU) nr. 575/2013 van het Europees Parlement en de Raad van 26 juni 2013 betreffende prudentiële vereisten voor kredietinstellingen en beleggingsondernemingen en tot wijziging van Verordening (EU) nr. 648/2012 (PB L 176 van 27.6.2013, blz. 1).

⁴⁷ Richtlijn 2008/48/EG van het Europees Parlement en de Raad van 23 april 2008 inzake kredietovereenkomsten voor consumenten en tot intrekking van Richtlijn 87/102/EEG van de Raad (PB L 133 van 22.5.2008, blz. 66).

⁴⁸ Richtlijn 2009/138/EG van het Europees Parlement en de Raad van 25 november 2009 betreffende de toegang tot en uitoefening van het verzekerings- en het herverzekeringsbedrijf (Solvabiliteit II) (PB L 335 van 17.12.2009, blz. 1).

⁴⁹ Richtlijn 2013/36/EU van het Europees Parlement en de Raad van 26 juni 2013 betreffende toegang tot het bedrijf van kredietinstellingen en het prudentieel toezicht op kredietinstellingen en beleggingsondernemingen, tot wijziging van Richtlijn 2002/87/EG en tot intrekking van de Richtlijnen 2006/48/EG en 2006/49/EG (PB L 176 van 27.6.2013, blz. 338).

⁵⁰ Richtlijn 2014/17/EU van het Europees Parlement en de Raad van 4 februari 2014 inzake kredietovereenkomsten voor consumenten met betrekking tot voor bewoning bestemde onroerende goederen en tot wijziging van de Richtlijnen 2008/48/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 (PB L 60 van 28.2.2014, blz. 34).

⁵¹ Richtlijn (EU) 2016/97 van het Europees Parlement en de Raad van 20 januari 2016 betreffende verzekeringsdistributie (PB L 26 van 2.2.2016, blz. 19).

Die bevoegde autoriteiten moeten over alle bevoegdheden uit hoofde van deze verordening en Verordening (EU) 2019/1020 beschikken om de eisen en verplichtingen van deze verordening te handhaven, met inbegrip van bevoegdheden om ex-postmarkttoezichtactiviteiten uit te voeren die, in voorkomend geval, kunnen worden geïntegreerd in hun bestaande toezichtsmechanismen en -procedures uit hoofde van het desbetreffende Unierecht inzake financiële diensten. Het is wenselijk te bepalen dat de nationale autoriteiten die verantwoordelijk zijn voor het toezicht op onder Richtlijn 2013/36/EU vallende kredietinstellingen en deelnemen aan het bij Verordening (EU) nr. 1024/2013 van de Raad⁵² ingestelde gemeenschappelijk toezichtsmechanisme, indien zij optreden als markttoezichtautoriteiten in het kader van deze verordening, alle bij hun markttoezichtactiviteiten verkregen informatie die potentieel van belang kan zijn voor de in die verordening omschreven taken van de Europese Centrale Bank met betrekking tot prudentieel toezicht onverwijld melden bij de Europese Centrale Bank. Teneinde de samenhang tussen deze verordening en de regels die van toepassing zijn op kredietinstellingen die vallen onder Richtlijn 2013/36/EU verder te verbeteren, is het ook passend om enkele van de procedurele verplichtingen van aanbieders in verband met risicobeheer, monitoring na het in de handel brengen en documentatie op te nemen in de bestaande verplichtingen en procedures in het kader van Richtlijn 2013/36/EU. Om overlappingen te voorkomen, moet ook worden voorzien in beperkte afwijkingen in verband met het systeem voor kwaliteitsbeheer van aanbieders en de monitorings-verplichting voor gebruiksverantwoordelijken van AI-systemen met een hoog risico voor zover deze van toepassing zijn op kredietinstellingen die vallen onder Richtlijn 2013/36/EU. Om te zorgen voor consistentie en gelijke behandeling in de financiële sector moet dezelfde regeling gelden voor verzekerings- en herverzekeringsondernemingen en verzekeringsholdings die vallen onder Richtlijn 2009/138/EG en verzekeringstussenpersonen die vallen onder Richtlijn (EU) 2016/97 en andere soorten financiële instellingen die gebonden zijn aan eisen inzake interne governance, regelingen of procedures die zijn vastgelegd op grond van het desbetreffende Unierecht inzake financiële diensten.

⁵² Verordening (EU) nr. 1024/2013 van de Raad van 15 oktober 2013 waarbij aan de Europese Centrale Bank specifieke taken worden opgedragen betreffende het beleid inzake het prudentieel toezicht op kredietinstellingen (PB L 287 van 29.10.2013, blz. 63).

- (159) Elke markttoezichtautoriteit voor AI-systemen met een hoog risico op het gebied van biometrische gegevens, zoals vermeld in een bijlage bij deze verordening, voor zover die systemen worden gebruikt voor rechtshandhaving, migratie, asiel en grenstoezichtsbeheer, of voor de rechtsbedeling en democratische processen, moet beschikken over doeltreffende onderzoeksbevoegdheden en corrigerende bevoegdheden, waaronder ten minste de bevoegdheid om toegang te verkrijgen tot alle persoonsgegevens die worden verwerkt en tot alle informatie die nodig is voor de uitvoering van haar taken. De markttoezichtautoriteiten moeten hun bevoegdheden volledig onafhankelijk kunnen uitoefenen. Eventuele beperkingen van hun toegang tot gevoelige operationele gegevens uit hoofde van deze verordening mogen geen afbreuk doen aan de hun bij Richtlijn (EU) 2016/680 verleende bevoegdheden. Geen enkele uitsluiting betreffende de openbaarmaking van gegevens aan nationale gegevensbeschermingsautoriteiten uit hoofde van deze verordening mag afbreuk doen aan de huidige of toekomstige bevoegdheden van die autoriteiten die buiten het toepassingsgebied van deze verordening vallen.
- (160) De markttoezichtautoriteiten en de Commissie moeten gezamenlijke activiteiten, waaronder gezamenlijke onderzoeken, kunnen voorstellen die door markttoezichtautoriteiten alleen of samen met de Commissie moeten worden uitgevoerd, met als doel de naleving te bevorderen, de niet-naleving vast te stellen, het bewustzijn te vergroten en richtsnoeren inzake deze verordening te verstrekken betreffende specifieke categorieën AI-systemen met een hoog risico die in twee of meer lidstaten een ernstig risico blijken te vormen. Gezamenlijke activiteiten ter bevordering van conformiteit moeten worden uitgevoerd overeenkomstig artikel 9 van Verordening (EU) 2019/1020. Het AI-bureau moet zorgen voor coördinerende ondersteuning van gezamenlijke onderzoeken.

(161) Het is noodzakelijk de verantwoordelijkheden en bevoegdheden op het niveau van de Unie en op nationaal niveau te verduidelijken wat betreft AI-systemen die gebaseerd zijn op AI-modellen voor algemene doeleinden. Om overlappende bevoegdheden te voorkomen, moet, indien een AI-systeem gebaseerd is op een AI-model voor algemene doeleinden en het model en systeem door dezelfde aanbieder worden aangeboden, het toezicht op het niveau van de Unie plaatsvinden via het AI-bureau, dat voor dit doel de bevoegdheden moet hebben van een markttoezichtautoriteit in de zin van Verordening (EU) 2019/1020. In alle andere gevallen blijven de nationale markttoezichtautoriteiten verantwoordelijk voor het toezicht op AI-systemen. Voor AI-systemen voor algemene doeleinden die rechtstreeks door gebruiksverantwoordelijken kunnen worden gebruikt voor ten minste één doel dat als hoog risico is geclassificeerd, moeten markttoezichtautoriteiten echter samenwerken met het AI-bureau om conformiteitsbeoordelingen uit te voeren en de AI-board en andere markttoezicht-autoriteiten daarvan in kennis te stellen. Voorts moeten markttoezichtautoriteiten het AI-bureau om bijstand kunnen verzoeken indien de markttoezichtautoriteit geen onderzoek naar een AI-systeem met een hoog risico kan afronden omdat zij geen toegang heeft tot bepaalde informatie met betrekking tot het AI-model voor algemene doeleinden waarop het AI-systeem met een hoog risico is gebaseerd. In dergelijke gevallen moet de procedure betreffende wederzijdse bijstand in grensoverschrijdende zaken van hoofdstuk VI van Verordening (EU) 2019/1020 op overeenkomstige wijze van toepassing zijn.

- (162) Om optimaal gebruik te maken van de gecentraliseerde Unie-expertise en van de synergieën op het niveau van de Unie, moeten de bevoegdheden voor het toezicht op en de handhaving van de verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden een bevoegdheid van de Commissie zijn. Het AI-bureau moet alle nodige maatregelen kunnen nemen om toezicht te houden op de doeltreffende uitvoering van deze verordening met betrekking tot AI-modellen voor algemene doeleinden. Het moet mogelijke inbreuken op de regels inzake aanbieders van AI-modellen voor algemene doeleinden kunnen onderzoeken, zowel op eigen initiatief, op basis van de resultaten van zijn monitoring-activiteiten, hetzij op verzoek van markttoezichtautoriteiten in overeenstemming met de in deze verordening vastgestelde voorwaarden. Om een doeltreffende monitoring van het AI-bureau te ondersteunen, moet het voorzien in de mogelijkheid dat aanbieders verder in de AI-waardeketen klachten indienen over mogelijke inbreuken op de regels inzake aanbieders van AI-modellen en -systemen voor algemene doeleinden.
- (163) Als aanvulling op de governance-systemen voor AI-modellen voor algemene doeleinden moet het wetenschappelijk panel de monitoring-activiteiten van het AI-bureau ondersteunen en kan het in bepaalde gevallen gekwalificeerde waarschuwingen aan het AI-bureau verstrekken die eventueel aanleiding geven tot vervolgonderzoeken. Dit moet het geval zijn indien het wetenschappelijk panel redenen heeft om te vermoeden dat een AI-model voor algemene doeleinden een concreet en aanwijsbaar risico op het niveau van de Unie vormt. Voorts moet dit het geval zijn indien het wetenschappelijk panel redenen heeft om te vermoeden dat een AI-model voor algemene doeleinden voldoet aan de criteria om als AI-model voor algemene doeleinden met een systeemrisico te worden geclassificeerd. Om het wetenschappelijk panel uit te rusten met de informatie die nodig is voor de uitvoering van die taken, moet er een mechanisme zijn waarbij het wetenschappelijk panel de Commissie kan verzoeken documentatie of informatie van een aanbieder te eisen.

- (164) Het AI-bureau moet de nodige maatregelen kunnen nemen om de doeltreffende uitvoering en naleving van de in deze verordening vastgestelde verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden te monitoren. Het AI-bureau moet mogelijke inbreuken kunnen onderzoeken overeenkomstig de bevoegdheden waarin deze verordening voorziet, onder meer door documentatie en informatie op te vragen, evaluaties uit te voeren en door aanbieders van AI-modellen voor algemene doeleinden om maatregelen te verzoeken. Om gebruik te maken van onafhankelijke expertise moet het AI-bureau bij de uitvoering van evaluaties onafhankelijke deskundigen kunnen betrekken om namens het bureau de evaluaties uit te voeren. Naleving van de verplichtingen moet afdwingbaar zijn, onder meer door verzoeken om passende maatregelen te nemen, met inbegrip van risicobeperkende maatregelen in het geval van vastgestelde systeemrisico's, alsook door het op de markt aanbieden van het model te beperken, het uit de handel te nemen of het terug te roepen. Als waarborg moeten aanbieders van AI-modellen voor algemene doeleinden, indien nodig naast de procedurele rechten waarin deze verordening voorziet, over de procedurele rechten beschikken waarin is voorzien in artikel 18 van Verordening (EU) 2019/1020, dat van overeenkomstige toepassing is, onverminderd specifiekere procedurele rechten waarin deze verordening voorziet.

(165) De ontwikkeling van andere AI-systemen dan AI-systemen met een hoog risico in overeenstemming met de eisen van deze verordening kan leiden tot een groter gebruik van ethische en betrouwbare AI in de Unie. Aanbieders van AI-systemen zonder hoog risico moeten worden aangemoedigd om gedragscodes op te stellen, met inbegrip van gerelateerde governancemechanismen, die bedoeld zijn ter bevordering van de vrijwillige toepassing van sommige of alle dwingende eisen die gelden voor AI-systemen met een hoog risico, aangepast in het licht van het beoogde doel van de systemen en het lagere risico ervan en rekening houdend met de beschikbare technische oplossingen en beste praktijken van de sector, zoals model- en gegevenskaarten. Aanbieders en, in voorkomend geval, gebruiksverantwoordelijken van alle AI-systemen, al dan niet met een hoog risico, en AI-modellen moeten ook worden aangemoedigd om op vrijwillige basis aanvullende eisen toe te passen, bijvoorbeeld met betrekking tot de elementen van de “ethische richtsnoeren van de Unie voor betrouwbare KI”, milieuduurzaamheid, maatregelen op het gebied van AI-geletterdheid, inclusief en divers ontwerp en ontwikkeling van AI-systemen, met inbegrip van aandacht voor kwetsbare personen en toegankelijkheid voor personen met een handicap, deelname van belanghebbenden, in voorkomend geval met betrokkenheid van relevante belanghebbenden zoals het bedrijfsleven en maatschappelijke organisaties, de academische wereld, onderzoeksorganisaties, vakbonden en consumentenorganisaties bij het ontwerp en de ontwikkeling van AI-systemen, en diversiteit van de ontwikkelingsteams, met inbegrip van genderevenwicht. Om ervoor te zorgen dat de vrijwillige gedragscodes doeltreffend zijn, moeten zij gebaseerd zijn op duidelijke doelstellingen en kernprestatie-indicatoren om de verwezenlijking van die doelstellingen te meten. Zij moeten in voorkomend geval ook op inclusieve wijze worden ontwikkeld, met betrokkenheid van relevante belanghebbenden zoals het bedrijfsleven en maatschappelijke organisaties, de academische wereld, onderzoeksorganisaties, vakbonden en consumentenorganisaties. De Commissie kan initiatieven ontwikkelen, ook van sectorale aard, om de technische belemmeringen voor grensoverschrijdende uitwisseling van data voor AI-ontwikkeling te helpen beperken, onder meer met betrekking tot infrastructuur voor de toegang tot data en de semantische en technische interoperabiliteit van verschillende soorten data.

- (166) Het is belangrijk dat AI-systemen die verband houden met producten en die overeenkomstig deze verordening geen hoog risico met zich meebrengen en derhalve niet hoeven te voldoen aan de eisen voor AI-systemen met een hoog risico, desalniettemin veilig zijn indien zij in de handel worden gebracht of in gebruik worden gesteld. Met het oog op deze doelstelling zou Verordening (EU) 2023/988 van het Europees Parlement en de Raad⁵³ als vangnet van toepassing zijn.
- (167) Om een betrouwbare en constructieve samenwerking van bevoegde autoriteiten op Unie- en nationaal niveau te waarborgen, moeten alle partijen die betrokken zijn bij de toepassing van deze verordening de vertrouwelijkheid eerbiedigen van informatie en data die zij bij de uitvoering van hun taken verkrijgen, overeenkomstig het Unierecht of het nationale recht. Zij moeten hun taken en activiteiten zodanig uitvoeren dat met name intellectuele-eigendomsrechten, vertrouwelijke bedrijfsinformatie en bedrijfsgeheimen, de doeltreffende uitvoering van deze verordening, openbare en nationale veiligheidsbelangen, de integriteit van strafrechtelijke en administratieve procedures en de integriteit van gerubriceerde informatie worden beschermd.

⁵³ Verordening (EU) 2023/988 van het Europees Parlement en de Raad van 10 mei 2023 inzake algemene productveiligheid, tot wijziging van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad en Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad, en tot intrekking van Richtlijn 2001/95/EG van het Europees Parlement en de Raad en Richtlijn 87/357/EEG van de Raad (PB L 135 van 23.5.2023, blz. 1).

- (168) Naleving van deze verordening moet afdwingbaar zijn door het opleggen van sancties en andere handhavingsmaatregelen. De lidstaten moeten alle nodige maatregelen treffen opdat de bepalingen van deze verordening worden uitgevoerd, onder meer door te voorzien in doeltreffende, evenredige en afschrikkende sancties bij inbreuken daarop, en opdat het beginsel non bis in idem in acht wordt genomen. Teneinde de administratieve sancties tegen inbreuken op deze verordening te versterken en te harmoniseren, moeten de maxima voor de vaststelling van de administratieve geldboeten voor bepaalde specifieke inbreuken worden vastgesteld. Bij de beoordeling van het bedrag van de boeten moeten de lidstaten per afzonderlijk geval rekening houden met alle relevante omstandigheden van de specifieke situatie, met inachtneming van met name de aard, de ernst en de duur van de inbreuk, de gevolgen ervan en de omvang van de aanbieder, met name indien de aanbieder een kmo is, met inbegrip van start-ups. De Europese Toezichthouder voor gegevensbescherming moet bevoegd zijn om boeten op te leggen aan instellingen, agentschappen en organen van de Unie die binnen het toepassingsgebied van deze verordening vallen.
- (169) De naleving van de uit hoofde van deze verordening opgelegde verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden moet onder meer afdwingbaar zijn door middel van boeten. Daartoe moeten ook passende boeten worden vastgesteld voor inbreuken op die verplichtingen, met inbegrip van de niet-naleving van de door de Commissie overeenkomstig deze verordening gevraagde maatregelen, met inachtneming van passende verjaringstermijnen overeenkomstig het evenredigheidsbeginsel. Alle besluiten die de Commissie krachtens deze verordening neemt, zijn overeenkomstig het VWEU onderworpen aan toetsing door het Hof van Justitie van de Europese Unie, met inbegrip van de onbeperkte rechtsmacht van het Hof van Justitie wat betreft sancties op grond van artikel 261 VWEU.

- (170) Het Unierecht en het nationale recht voorzien reeds in doeltreffende rechtsmiddelen voor natuurlijke personen en rechtspersonen van wie de rechten en vrijheden worden geschaad door het gebruik van AI-systemen. Onverminderd die rechtsmiddelen, kan elke natuurlijke of rechtspersoon die redenen heeft om aan te nemen dat er sprake is van een inbreuk op de bepalingen van deze verordening, een met redenen omklede klacht indienen bij de betrokken markttoezichtautoriteit.
- (171) Getroffen personen moeten het recht hebben om uitleg te krijgen indien het besluit van een gebruiksverantwoordelijke voornamelijk is gebaseerd op de output van bepaalde AI-systemen met een hoog risico die binnen het toepassingsgebied van deze verordening vallen en indien dat besluit rechtsgevolgen of gelijkaardige aanzienlijke gevolgen heeft voor de gezondheid, veiligheid of grondrechten van die personen. Die uitleg moet duidelijk en zinvol zijn en moet de grondslag zijn waarop de getroffen personen zich kunnen baseren om hun rechten uit te oefenen. Het recht om uitleg te krijgen mag niet van toepassing zijn op het gebruik van AI-systemen waarvoor uitzonderingen of beperkingen voortvloeien uit het Unierecht of het nationale recht en moet alleen van toepassing zijn voor zover het Unierecht niet reeds in dit recht voorziet.
- (172) Personen die optreden als klokkenluiders bij inbreuken op deze verordening, moeten worden beschermd uit hoofde van het Unierecht. Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad⁵⁴ moet daarom van toepassing zijn op de melding van inbreuken op deze verordening en op de bescherming van personen die dergelijke inbreuken melden.

⁵⁴ Richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (PB L 305 van 26.11.2019, blz. 17).

(173) Om ervoor te zorgen dat het regelgevingskader waar nodig kan worden aangepast, moet aan de Commissie de bevoegdheid worden overgedragen om overeenkomstig artikel 290 VWEU handelingen vast te stellen tot wijziging van de voorwaarden waaronder een AI-systeem niet als een AI-systeem met een hoog risico wordt beschouwd, van de lijst van AI-systemen met een hoog risico, van de bepalingen inzake technische documentatie, van de inhoud van de EU-conformiteitsverklaring, van de bepalingen betreffende de conformiteitsbeoordelingsprocedures, van de bepalingen tot vaststelling van AI-systemen met een hoog risico waarop de conformiteitsbeoordelingsprocedure op basis van de beoordeling van het kwaliteitsbeheersysteem en de beoordeling van de technische documentatie moet gelden, van de drempel, benchmarks en indicatoren, onder meer door die benchmarks en indicatoren aan te vullen, van de regels voor de classificatie van AI-modellen voor algemene doeleinden met systeemrisico's, van de criteria voor de aanwijzing van AI-modellen voor algemene doeleinden met een systeemrisico, van de technische documentatie voor aanbieders van AI-modellen voor algemene doeleinden en van de transparantie-informatie voor aanbieders van AI-modellen voor algemene doeleinden. Het is van bijzonder belang dat de Commissie bij haar voorbereidende werkzaamheden tot passende raadplegingen overgaat, onder meer op deskundigenniveau, en dat die raadplegingen gebeuren in overeenstemming met de beginselen die zijn vastgelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven⁵⁵. Met name om te zorgen voor gelijke deelname aan de voorbereiding van gedelegeerde handelingen, ontvangen het Europees Parlement en de Raad alle documenten op hetzelfde tijdstip als de deskundigen van de lidstaten, en hebben hun deskundigen systematisch toegang tot de vergaderingen van de deskundigengroepen van de Commissie die zich bezighouden met de voorbereiding van de gedelegeerde handelingen.

⁵⁵ PB L 123 van 12.5.2016, blz. 1.

(174) Gezien de snelle technologische ontwikkelingen en de technische deskundigheid die vereist is om deze verordening doeltreffende toe te passen, moet de Commissie deze verordening uiterlijk op ... [vijf jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de vier jaar evalueren en toetsen en verslag uitbrengen aan het Europees Parlement en de Raad. Daarnaast moet de Commissie, rekening houdend met de gevolgen voor het toepassingsgebied van deze verordening, eenmaal per jaar een beoordeling uitvoeren van de noodzaak om de lijst van AI-systemen met een hoog risico en de lijst van verboden praktijken te wijzigen. Bovendien moet de Commissie uiterlijk op ... [vier jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de vier jaar een evaluatie maken van de noodzaak om de lijst van rubrieken van gebieden met een hoog risico in de bijlage bij deze verordening te wijzigen, van de AI-systemen die onder de transparantieverplichtingen vallen en van de doeltreffendheid van het toezicht- en governancesysteem en de vooruitgang bij de ontwikkeling van normalisatieproducten met betrekking tot de energie-efficiënte ontwikkeling van AI-modellen voor algemene doeleinden, met inbegrip van de behoefte aan verdere maatregelen of acties, en hierover verslag uitbrengen aan het Europees Parlement en de Raad. Tot slot moet de Commissie uiterlijk op ... [vier jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de drie jaar de impact en de doeltreffendheid evalueren van vrijwillige gedragscodes om de toepassing van de eisen voor AI-systemen met een hoog risico op andere AI-systemen dan AI-systemen met een hoog risico te bevorderen, en eventuele andere aanvullende eisen voor dergelijke AI-systemen.

- (175) Om eenvormige voorwaarden te waarborgen voor de uitvoering van deze verordening, moeten aan de Commissie uitvoeringsbevoegdheden worden toegekend. Die bevoegdheden moeten worden uitgeoefend in overeenstemming met Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad⁵⁶.
- (176) Aangezien de doelstelling van deze verordening, namelijk het verbeteren van de werking van de interne markt en het bevorderen van de invoering van mensgerichte en betrouwbare AI, waarbij tegelijkertijd een hoog niveau van bescherming van de gezondheid, de veiligheid en de in het Handvest verankerde grondrechten wordt gewaarborgd, met inbegrip van de democratie, de rechtsstaat en de bescherming van het milieu tegen de schadelijke gevolgen van AI-systemen in de Unie en het ondersteunen van innovatie, niet voldoende door de lidstaten kan worden verwezenlijkt en vanwege de omvang of de gevolgen van het optreden beter op het niveau van de Unie kan worden verwezenlijkt, kan de Unie, overeenkomstig het in artikel 5 VEU neergelegde subsidiariteitsbeginsel, maatregelen nemen. Overeenkomstig het in hetzelfde artikel neergelegde evenredigheidsbeginsel gaat deze verordening niet verder dan nodig is om deze doelstelling te verwezenlijken.

⁵⁶ Verordening (EU) nr. 182/2011 van het Europees Parlement en de Raad van 16 februari 2011 tot vaststelling van de algemene voorschriften en beginselen die van toepassing zijn op de wijze waarop de lidstaten de uitoefening van de uitvoeringsbevoegdheden door de Commissie controleren (PB L 55 van 28.2.2011, blz. 13).

- (177) Om rechtszekerheid te waarborgen, ervoor te zorgen dat er een passende aanpassingsperiode is voor operatoren en verstoring van de markt te voorkomen, onder meer door de continuïteit van het gebruik van AI-systemen te waarborgen, is het wenselijk dat AI-systemen met een hoog risico die vóór de algemene datum van toepassing van deze verordening in de handel zijn gebracht of in gebruik zijn gesteld enkel onderworpen zijn aan deze verordening indien hun ontwerp of beoogde doel na die datum aanzienlijk is gewijzigd. Er moet worden verduidelijkt dat een aanzienlijke wijziging in dit verband inhoudelijk overeenkomt met het begrip substantiële wijziging, dat enkel wordt gebruikt met betrekking tot AI-systemen met een hoog risico op grond van deze verordening. Bij wijze van uitzondering en in het licht van de publieke verantwoordingsplicht moeten operatoren van AI-systemen die componenten zijn van de grootschalige IT-systemen die zijn opgezet volgens de in een bijlage bij deze verordening vermelde rechtshandelingen, en operatoren van AI-systemen met een hoog risico die bedoeld zijn om door overheidsinstanties te worden gebruikt, respectievelijk uiterlijk eind 2030 en uiterlijk op ... [zes jaar na de datum van inwerkingtreding van deze verordening] de nodige stappen nemen om aan de eisen ervan te voldoen.
- (178) Aanbieders van AI-systemen met een hoog risico worden aangemoedigd de desbetreffende verplichtingen van deze verordening al tijdens de overgangsperiode op vrijwillige basis toe te passen.

(179) Deze verordening moet van toepassing zijn met ingang van ... [twee jaar na de datum van inwerkingtreding van deze verordening]. Rekening houdend met het onaanvaardbare risico in verband met de manier waarop AI soms kan worden gebruikt, moeten de verbodsbepalingen alsmede de algemene bepalingen van deze verordening echter reeds van toepassing zijn met ingang van ... [zes maanden na de datum van inwerkingtreding van deze verordening]. Hoewel het volledige resultaat van die verbodsbepalingen pas zichtbaar wordt met de governance en de handhaving van deze verordening, is het van belang op de toepassing van deze verbodsbepalingen te anticiperen om rekening te houden met onaanvaardbare risico's en om een weerslag te hebben op andere procedures, zoals in het burgerlijk recht. Voorts moet de infrastructuur in verband met de governance en het systeem voor de conformiteitsbeoordeling vóór ... [twee jaar na de datum van inwerkingtreding van deze verordening] operationeel zijn en moeten de bepalingen inzake aangemelde instanties en de governancestructuur derhalve van toepassing zijn vanaf ... [12 maanden na de datum van inwerkingtreding van deze verordening]. Gezien het snelle tempo van de technologische vooruitgang en de invoering van AI-modellen voor algemene doeleinden, moeten de verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden van toepassing zijn met ingang van ... [12 maanden na de datum van inwerkingtreding van deze verordening]. Praktijkcodes moeten uiterlijk op ... [9 maanden na de datum van inwerkingtreding van deze verordening] gereed zijn om aanbieders in staat te stellen de naleving ervan tijdig aan te tonen. Het AI-bureau moet ervoor zorgen dat de classificatieregels en -procedures actueel zijn in het licht van technologische ontwikkelingen. De lidstaten moeten daarnaast de regels inzake sancties, waaronder administratieve geldboeten, vaststellen en de Commissie hiervan in kennis stellen en ervoor zorgen dat deze uiterlijk op de datum van toepassing van deze verordening naar behoren en op doeltreffende wijze worden uitgevoerd. De bepalingen inzake sancties moeten met ingang van ... [12 maanden na de datum van de inwerkingtreding van deze verordening] van toepassing zijn.

- (180) Overeenkomstig artikel 42, leden 1 en 2, van Verordening (EU) 2018/1725 zijn de Europese Toezichthouder voor gegevensbescherming en het Europees Comité voor gegevensbescherming geraadpleegd, en op 18 juni 2021 hebben zij hun gezamenlijk advies uitgebracht,

HEBBEN DE VOLGENDE VERORDENING VASTGESTELD:

Hoofdstuk I

Algemene bepalingen

Artikel 1

Onderwerp

1. Deze verordening heeft tot doel de werking van de interne markt te verbeteren en de toepassing van mensgerichte en betrouwbare artificiële intelligentie (AI) te bevorderen, en tegelijkertijd een hoog niveau van bescherming van de gezondheid, de veiligheid en de in het Handvest verankerde grondrechten te waarborgen, met inbegrip van de democratie, de rechtsstaat en de bescherming van het milieu, tegen de schadelijke gevolgen van AI-systemen in de Unie, en innovatie te ondersteunen.
2. Bij deze verordening worden vastgesteld:
 - a) geharmoniseerde regels voor het in de handel brengen, in gebruik stellen en gebruiken van AI-systemen in de Unie;
 - b) een verbod op bepaalde AI-praktijken;
 - c) specifieke eisen voor AI-systemen met een hoog risico en verplichtingen voor de operatoren van dergelijke systemen;
 - d) geharmoniseerde transparantievoorschriften voor bepaalde AI-systemen;
 - e) geharmoniseerde regels voor het in de handel brengen van AI-modellen voor algemene doeleinden;

- f) regels inzake marktmonitoring, markttoezicht, governance en handhaving van die regels;
- g) maatregelen ter ondersteuning van innovatie, met bijzondere nadruk op kmo's, waaronder start-ups.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op:
 - a) aanbieders die AI-systemen in de Unie in de handel brengen of in gebruik stellen, of AI-modellen voor algemene doeleinden in de handel brengen, ongeacht of deze aanbieders in de Unie of in een derde land zijn gevestigd of er zich bevinden;
 - b) gebruiksverantwoordelijken van AI-systemen die in de Unie zijn gevestigd of er zich bevinden;
 - c) aanbieders en gebruiksverantwoordelijken van AI-systemen die in een derde land zijn gevestigd of er zich bevinden, indien de output van het AI-systeem in de Unie wordt gebruikt;
 - d) importeurs en distributeurs van AI-systemen;
 - e) fabrikanten van producten die samen met hun product en onder hun eigen naam of merk een AI-systeem in de handel brengen of in gebruik stellen;
 - f) gemachtigden van aanbieders die niet in de Unie gevestigd zijn;
 - g) getroffen personen die zich in de Unie bevinden.

2. Op AI-systemen die overeenkomstig artikel 6, lid 1, als AI-systemen met een hoog risico worden aangemerkt die verband houden met producten die vallen onder de in bijlage I, afdeling B, opgenomen harmonisatiewetgeving van de Unie, zijn uitsluitend artikel 6, lid 1, de artikelen 102 tot en met 109 en artikel 112 van toepassing. Artikel 57 is alleen van toepassing voor zover de eisen voor AI-systemen met een hoog risico uit hoofde van deze verordening zijn opgenomen in die harmonisatiewetgeving van de Unie.
3. Deze verordening is niet van toepassing op gebieden die buiten het toepassingsgebied van het Unierecht vallen en doet in geen geval afbreuk aan de bevoegdheden van de lidstaten op het gebied van nationale veiligheid, ongeacht het soort entiteit dat door de lidstaten is belast met de uitvoering van taken in verband met die bevoegdheden.

Deze verordening is niet van toepassing op AI-systemen wanneer en in zover die uitsluitend in de handel worden gebracht, in gebruik worden gesteld of, al dan niet gewijzigd, worden gebruikt voor militaire, defensie- of nationale veiligheidsdoeleinden, ongeacht het soort entiteit dat deze activiteiten uitvoert.

Deze verordening is niet van toepassing op AI-systemen die niet in de Unie in de handel worden gebracht of in gebruik worden gesteld en waarvan de output in de Unie uitsluitend wordt gebruikt voor militaire, defensie- of nationale veiligheidsdoeleinden, ongeacht het soort entiteit dat deze activiteiten uitvoert.

4. Deze verordening is niet van toepassing op overheidsinstanties in derde landen of internationale organisaties die op grond van lid 1 binnen het toepassingsgebied van deze verordening vallen, wanneer deze instanties of organisaties AI-systemen gebruiken in het kader van internationale samenwerking of overeenkomsten met de Unie of een of meer lidstaten op het gebied van rechtshandhaving en justitie, op voorwaarde dat een dergelijk derde land of internationale organisatie passende waarborgen biedt met betrekking tot de bescherming van de grondrechten en fundamentele vrijheden van natuurlijke personen.
5. Deze verordening laat de toepassing van de bepalingen inzake de aansprakelijkheid van aanbieders van tussenhandelsdiensten als vastgelegd in hoofdstuk II van Verordening (EU) 2022/2065 onverlet.
6. Deze verordening is niet van toepassing op AI-systemen of AI-modellen, met inbegrip van hun output, die specifiek zijn ontwikkeld en in gebruik gesteld met wetenschappelijk onderzoek en wetenschappelijke ontwikkeling als enig doel.
7. Het Unierecht inzake de bescherming van persoonsgegevens, de privacy en de vertrouwelijkheid van communicatie is van toepassing op persoonsgegevens die worden verwerkt in verband met de rechten en verplichtingen die in deze verordening zijn vastgelegd. Deze verordening laat de Verordeningen (EU) 2016/679 of (EU) 2018/1725, of de Richtlijnen 2002/58/EG of (EU) 2016/680 onverlet, onverminderd artikel 10, lid 5, en artikel 59 van deze verordening.
8. Deze verordening is niet van toepassing op onderzoeks-, test- of ontwikkelingsactiviteiten met betrekking tot AI-systemen of AI-modellen voor zij in de handel worden gebracht of in gebruik worden gesteld. Dergelijke activiteiten worden uitgevoerd in overeenstemming met het toepasselijke Unierecht. Testen onder reële omstandigheden vallen niet onder die uitsluiting.

9. Deze verordening doet geen afbreuk aan de regels die zijn vastgelegd in andere rechtshandelingen van de Unie betreffende consumentenbescherming en productveiligheid.
10. Deze verordening is niet van toepassing op verplichtingen van gebruiksverantwoordelijken die natuurlijke personen zijn die AI-systemen gebruiken in het kader van een louter persoonlijke niet-professionele activiteit.
11. Deze verordening belet de Unie of de lidstaten niet om wettelijke of bestuursrechtelijke bepalingen te handhaven of in te voeren die gunstiger zijn voor werknemers wat betreft de bescherming van hun rechten met betrekking tot het gebruik van AI-systemen door werkgevers, of om de toepassing van voor werknemers gunstigere collectieve overeenkomsten aan te moedigen of toe te staan.
12. Deze verordening is niet van toepassing op AI-systemen die worden vrijgegeven onder vrije en opensourcelicenties, tenzij zij in de handel worden gebracht of in gebruik worden gesteld als AI-systemen met een hoog risico of als een AI-systeem dat onder artikel 5 of 50 valt.

Artikel 3

Definities

Voor de toepassing van deze verordening wordt verstaan onder:

- 1) “AI-systeem”: een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen;

- 2) “risico”: de combinatie van de kans op schade en de ernst van die schade;
- 3) “aanbieder”: een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem of een AI-model voor algemene doeleinden ontwikkelt of laat ontwikkelen en dat systeem of model in de handel brengt of het AI-systeem in gebruik stelt onder de eigen naam of merk, al dan niet tegen betaling;
- 4) “gebruiksverantwoordelijke”: een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem onder eigen verantwoordelijkheid gebruikt, tenzij het AI-systeem wordt gebruikt in het kader van een persoonlijke niet-beroepsactiviteit;
- 5) “gemachtigde”: een natuurlijke of rechtspersoon die zich bevindt of gevestigd is in de Unie die een schriftelijke machtiging heeft gekregen en aanvaard van een aanbieder van een AI-systeem of een AI-model voor algemene doeleinden om namens die aanbieder de verplichtingen en procedures van deze verordening respectievelijk na te komen en uit te voeren;
- 6) “importeur”: een natuurlijke of rechtspersoon die zich bevindt of gevestigd is in de Unie die een AI-systeem in de handel brengt dat de naam of het merk van een in een derde land gevestigde natuurlijke of rechtspersoon draagt;
- 7) “distributeur”: een andere natuurlijke persoon of rechtspersoon in de toeleveringsketen dan de aanbieder of de importeur, die een AI-systeem in de Unie op de markt aanbiedt;
- 8) “operator”: een aanbieder, productfabrikant, gebruiksverantwoordelijke, gemachtigde, importeur of distributeur;

- 9) “in de handel brengen”: het voor het eerst in de Unie op de markt aanbieden van een AI-systeem of een AI-model voor algemene doeleinden;
- 10) “op de markt aanbieden”: het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van een AI-systeem of een AI-model voor algemene doeleinden met het oog op distributie of gebruik op de markt van de Unie;
- 11) “in gebruik stellen”: de directe levering van een AI-systeem aan de gebruiksverantwoordelijke voor het eerste gebruik of voor eigen gebruik in de Unie voor het beoogde doel;
- 12) “beoogd doel”: het gebruik waarvoor een AI-systeem door de aanbieder is bedoeld, met inbegrip van de specifieke context en voorwaarden van het gebruik, zoals gespecificeerd in de informatie die door de aanbieder in de gebruiksinstructies, reclame- of verkoopmaterialen en verklaringen, alsook in de technische documentatie is verstrekt;
- 13) “redelijkerwijs te voorzien misbruik”: het gebruik van een AI-systeem op een wijze die niet in overeenstemming is met het beoogde doel, maar die kan voortvloeien uit redelijkerwijs te voorzien menselijk gedrag of redelijkerwijs te voorziene interactie met andere systemen, waaronder andere AI-systemen;
- 14) “veiligheidscomponent”: een component van een product of van een AI-systeem die een veiligheids-functie voor dat product of AI-systeem vervult of waarvan het falen of gebrekkig functioneren de gezondheid en veiligheid van personen of eigendom in gevaar brengt;
- 15) “gebruiksaanwijzingen”: de door de aanbieder verstrekte informatie om de gebruiksverantwoordelijke te informeren over met name het beoogde doel en juiste gebruik van een AI-systeem;

- 16) “terugroepen van een AI-systeem”: een maatregel gericht op het retourneren aan de aanbieder, het buiten gebruik stellen of het onbruikbaar maken van een AI-systeem dat aan gebruiksverantwoordelijken ter beschikking is gesteld;
- 17) “uit de handel nemen van een AI-systeem”: een maatregel waarmee wordt beoogd te voorkomen dat een AI-systeem dat zich in de toeleveringsketen bevindt, op de markt wordt aangeboden;
- 18) “prestaties van een AI-systeem”: het vermogen van een AI-systeem om het beoogde doel te verwezenlijken;
- 19) “aanmeldende autoriteit”: de nationale autoriteit die verantwoordelijk is voor het opzetten en uitvoeren van de noodzakelijke procedures voor de beoordeling, aanwijzing en kennisgeving van de conformiteitsbeoordelingsinstanties en de monitoring hiervan;
- 20) “conformiteitsbeoordeling”: het proces waarbij de naleving wordt aangetoond van de voorschriften van hoofdstuk III, afdeling 2, in verband met een AI-systeem met een hoog risico;
- 21) “conformiteitsbeoordelingsinstantie”: een instantie die als derde partij conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer testen, certificeren en inspecteren;
- 22) “aangemelde instantie”: een conformiteitsbeoordelingsinstantie die overeenkomstig deze verordening en andere relevante harmonisatiewetgeving van de Unie, is aangemeld;
- 23) “substantiële wijziging”: een verandering van een AI-systeem nadat dit in de handel is gebracht of in gebruik is gesteld, die door de aanbieder niet is voorzien of gepland in de initiële conformiteitsbeoordeling en als gevolg waarvan de overeenstemming van het AI-systeem met de voorschriften van hoofdstuk III, afdeling 2, wordt beïnvloed, of die leidt tot een wijziging van het beoogde doel waarvoor het AI-systeem is beoordeeld;

- 24) “CE-markering”: een markering waarmee een aanbieder aangeeft dat een AI-systeem in overeenstemming is met de voorschriften van hoofdstuk III, afdeling 2, en andere toepasselijke harmonisatiewetgeving van de Unie, die in het aanbrengen ervan voorzien;
- 25) “systeem voor monitoring na het in de handel brengen”: alle door aanbieders van AI-systemen verrichte activiteiten voor het verzamelen en evalueren van ervaringen met door hen in de handel gebrachte of in gebruik gestelde AI-systemen, teneinde te kunnen vaststellen of er onmiddellijk corrigerende dan wel preventieve maatregelen nodig zijn;
- 26) “markttoezichtautoriteit”: de nationale autoriteit die de activiteiten verricht en maatregelen neemt als bedoeld in Verordening (EU) 2019/1020;
- 27) “geharmoniseerde norm”: een geharmoniseerde norm zoals gedefinieerd in artikel 2, lid 1, punt c), van Verordening (EU) nr. 1025/2012;
- 28) “gemeenschappelijke specificatie”: een reeks technische specificaties zoals gedefinieerd in artikel 2, punt 4, van Verordening (EU) nr. 1025/2012, om te voldoen aan bepaalde voorschriften zoals vastgelegd in deze verordening;
- 29) “trainingsdata”: data die worden gebruikt voor het trainen van een AI-systeem door de leerbare parameters hiervan aan te passen;
- 30) “validatiedata”: data die worden gebruikt voor het verrichten van een evaluatie van het getrainde AI-systeem en voor het afstemmen van onder andere de niet-leerbare parameters en het leerproces ervan, om underfitting of overfitting te voorkomen;

- 31) “validatiedataset”: een afzonderlijke dataset of deel van de trainingsdataset, als vaste of variabele opdeling;
- 32) “testdata”: data die worden gebruikt voor het verrichten van een onafhankelijke evaluatie van het AI-systeem om de verwachte prestaties van dat systeem te bevestigen voordat het in de handel wordt gebracht of in gebruik wordt gesteld;
- 33) “inputdata”: data die in een AI-systeem worden ingevoerd of direct door een AI-systeem worden verworven en op basis waarvan het systeem een output genereert;
- 34) “biometrische gegevens”: persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijk persoon, zoals gezichtsafbeeldingen of vingerafdrukgegevens;
- 35) “biometrische identificatie”: de geautomatiseerde herkenning van fysieke, fysiologische, gedragsgerelateerde of psychologische menselijke kenmerken om de identiteit van een natuurlijk persoon vast te stellen door biometrische gegevens van die persoon te vergelijken met in een databank opgeslagen biometrische gegevens van personen;
- 36) “biometrische verificatie”: de geautomatiseerde één-op-éénverificatie, met inbegrip van de authenticatie, van de identiteit van natuurlijke personen door hun biometrische gegevens te vergelijken met eerder verstrekte biometrische gegevens;
- 37) “bijzondere categorieën persoonsgegevens”: de categorieën persoonsgegevens als bedoeld in artikel 9, lid 1, van Verordening (EU) 2016/679, artikel 10 van Richtlijn (EU) 2016/680 en artikel 10, lid 1, van Verordening (EU) 2018/1725;

- 38) “gevoelige operationele gegevens”: operationele gegevens met betrekking tot activiteiten op het gebied van preventie, opsporing, onderzoek of vervolging van strafbare feiten waarvan de openbaarmaking de integriteit van strafprocedures in het gedrang zou kunnen brengen;
- 39) “systeem voor het herkennen van emoties”: een AI-systeem dat is bedoeld voor het vaststellen of afleiden van de emoties of intenties van natuurlijke personen op basis van hun biometrische gegevens;
- 40) “systeem voor biometrische categorisering” een AI-systeem dat is bedoeld voor het indelen van natuurlijke personen in specifieke categorieën op basis van hun biometrische gegevens, tenzij dit een aanvulling vormt op een andere commerciële dienst en om objectieve technische redenen strikt noodzakelijk is;
- 41) “systeem voor biometrische identificatie op afstand”: een AI-systeem dat is bedoeld voor het identificeren van natuurlijke personen, zonder dat zij daar actief bij betrokken zijn en doorgaans van een afstand, door middel van vergelijking van de biometrische gegevens van een persoon met de biometrische gegevens die zijn opgenomen in een referentiedatabank;
- 42) “systeem voor biometrische identificatie op afstand in real time”: een systeem voor biometrische identificatie op afstand, waarbij het vastleggen van biometrische gegevens, de vergelijking en de identificatie zonder significante vertraging plaatsvinden, zowel wanneer de identificatie niet enkel onmiddellijk plaatsvindt, maar ook wanneer de identificatie met beperkte korte vertragingen plaatsvindt, om omzeiling te voorkomen;
- 43) “systeem voor biometrische identificatie op afstand achteraf”: een ander biometrisch systeem voor de identificatie op afstand dan een systeem voor biometrische identificatie op afstand in real time;

- 44) “openbare ruimte”: een fysieke plek die in publieke of private handen is en toegankelijk is voor een onbepaald aantal natuurlijke personen, ongeacht of bepaalde voorwaarden voor de toegang van toepassing zijn, en ongeacht eventuele capaciteitsbeperkingen;
- 45) “rechtshandhavingsinstantie”:
- a) iedere overheidsinstantie die bevoegd is voor de voorkoming van, het onderzoek naar, de opsporing en de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; of
 - b) ieder ander orgaan dat of iedere andere entiteit die krachtens het recht van de lidstaten is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming van, het onderzoek naar, de opsporing en de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
- 46) “rechtshandhaving”: activiteiten die worden verricht door of namens rechtshandhavingsinstanties met het oog op de voorkoming van, het onderzoek naar, de opsporing of de vervolging van strafbare feiten of de uitvoering van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;
- 47) “AI-bureau”: de taak van de Commissie waarbij zij bijdraagt aan de uitvoering van, de monitoring van en het toezicht op AI-systemen en AI-modellen voor algemene doeleinden, en AI-governance, als bepaald in het besluit van de Commissie van 24 januari 2024; verwijzingen in deze verordening naar het AI-bureau worden begrepen als verwijzingen naar de Commissie;

- 48) “nationale bevoegde autoriteit”: een aanmeldende autoriteit of een de markttoezichtautoriteit; wat betreft AI-systemen die door instellingen, organen en instanties van de EU in gebruik worden gesteld of worden gebruikt, worden verwijzingen naar nationale bevoegde autoriteiten of markttoezichtautoriteiten in deze verordening begrepen als verwijzingen naar de Europese Toezichthouder voor gegevensbescherming;
- 49) “ernstig incident”: een incident of gebrekkig functioneren van een AI-systeem dat direct of indirect leidt tot:
- a) het overlijden van een persoon of ernstige schade voor de gezondheid van een persoon;
 - b) een ernstige en onomkeerbare verstoring van het beheer of de exploitatie van kritieke infrastructuur;
 - c) een schending van de uit het recht van de Unie voortvloeiende verplichtingen ter bescherming van de grondrechten;
 - d) ernstige schade aan eigendommen of het milieu;
- 50) “persoonsgegevens”: persoonsgegevens zoals gedefinieerd in artikel 4, punt 1, van Verordening (EU) 2016/679;
- 51) “niet-persoonsgebonden gegevens”: andere gegevens dan persoonsgegevens zoals gedefinieerd in artikel 4, punt 1, van Verordening (EU) 2016/679;
- 52) “profilering”: profilering zoals gedefinieerd in artikel 4, punt 4, van Verordening (EU) 2016/679;

- 53) “plan voor testen onder reële omstandigheden”: een document waarin de doelstellingen, methode, geografische reikwijdte, betrokken personen, duur, monitoring, organisatie en wijze van uitvoering van een test onder reële omstandigheden worden omschreven;
- 54) “testomgevingsplan”: tussen de deelnemende aanbieder en de bevoegde autoriteit overeengekomen document waarin de doelstellingen, de voorwaarden, het tijdschema, de methode en de vereisten voor de in de testomgeving uitgevoerde activiteiten worden beschreven;
- 55) “AI-testomgeving voor regelgeving”: een door een bevoegde autoriteit opgezet gecontroleerd kader dat aanbieders of toekomstige aanbieders van AI-systemen de mogelijkheid biedt een innovatief AI-systeem te ontwikkelen, trainen, valideren en testen, zo nodig onder reële omstandigheden, volgens een testomgevingsplan, voor een beperkte periode en onder begeleiding van een toezichthouder;
- 56) “AI-geletterdheid”: vaardigheden, kennis en begrip die aanbieders, gebruiksverantwoordelijken en betrokken personen, rekening houdend met hun respectieve rechten en plichten in het kader van deze verordening, in staat stellen geïnformeerd AI-systemen in te zetten en zich bewuster te worden van de kansen en risico’s van AI en de mogelijke schade die zij kan veroorzaken;
- 57) “testen onder reële omstandigheden”: het tijdelijk testen van een AI-systeem voor zijn beoogde doel onder reële omstandigheden buiten een laboratorium of anderszins gesimuleerde omgeving teneinde betrouwbare en robuuste gegevens te verkrijgen, en te beoordelen en te verifiëren of het AI-systeem overeenstemt met de voorschriften van deze verordening en het wordt niet aangemerkt als het in de handel brengen of in gebruik stellen van het AI-systeem in de zin van deze verordening, mits aan alle in artikel 57 of 60 vastgestelde voorwaarden is voldaan;

- 58) “proefpersoon” in het kader van tests onder reële omstandigheden: een natuurlijk persoon die deelneemt aan een test onder reële omstandigheden;
- 59) “geïnformeerde toestemming”: de vrijelijk gegeven, specifieke, ondubbelzinnige en vrijwillige uiting door een proefpersoon van zijn of haar bereidheid deel te nemen aan een bepaalde test onder reële omstandigheden, na geïnformeerd te zijn over alle aspecten van de test die van belang zijn voor zijn of haar beslissing om deel te nemen;
- 60) “deepfake”: door AI gegenereerd of gemanipuleerd beeld-, audio- of videomateriaal dat een gelijkenis vertoont met bestaande personen, voorwerpen, plaatsen, entiteiten of gebeurtenissen, en door een persoon ten onrechte voor authentiek of waarheidsgetrouw zou worden aangezien;
- 61) “wijdverbreide inbreuk”: alle handelingen of omissies die in strijd zijn met het Unierecht ter bescherming van de belangen van natuurlijke personen, waarbij:
- a) schade is veroorzaakt of waarschijnlijk zal worden veroorzaakt aan de collectieve belangen van natuurlijke personen met verblijfplaats in ten minste twee andere lidstaten dan de lidstaat waar:
 - i) de handeling of ommissie haar oorsprong vond of plaatshad;
 - ii) de betrokken aanbieder of, waar van toepassing, diens gemachtigde zich bevindt of is gevestigd; of
 - iii) de gebruiksverantwoordelijke is gevestigd, indien de inbreuk door de gebruiksverantwoordelijke is gepleegd;

- b) schade is veroorzaakt, wordt veroorzaakt of waarschijnlijk zal worden veroorzaakt aan de collectieve belangen van natuurlijke personen, en die gemeenschappelijke kenmerken hebben, waaronder dezelfde onrechtmatige praktijk of een inbreuk op hetzelfde belang, en die zich gelijktijdig voordoen en door dezelfde operator worden begaan in ten minste drie lidstaten;
- 62) “kritieke infrastructuur”: kritieke infrastructuur zoals gedefinieerd in artikel 2, punt 4, van Richtlijn (EU) 2022/2557;
- 63) “AI-model voor algemene doeleinden”: een AI-model, ook wanneer het is getraind met een grote hoeveelheid data met behulp van self-supervision op grote schaal, dat een aanzienlijk algemeen karakter vertoont en in staat is op competente wijze een breed scala aan verschillende taken uit te voeren, ongeacht de wijze waarop het model in de handel wordt gebracht, en dat kan worden geïntegreerd in een verscheidenheid aan systemen verder in de AI-waardeketen of toepassingen verder in de AI-waardeketen, met uitzondering van AI-modellen die worden gebruikt voor onderzoek, ontwikkeling of prototypingactiviteiten alvorens zij in de handel worden gebracht;
- 64) “capaciteiten met een grote impact”: capaciteiten die overeenkomen met of groter zijn dan de capaciteiten die worden opgetekend bij de meest geavanceerde AI-modellen voor algemene doeleinden;
- 65) “systeemrisico”: een risico dat specifiek is voor de capaciteiten met een grote impact van AI-modellen voor algemene doeleinden, die aanzienlijke gevolgen hebben voor de markt van de Unie vanwege hun bereik, of vanwege feitelijke of redelijkerwijs te voorzien negatieve gevolgen voor de gezondheid, de veiligheid, de openbare veiligheid, de grondrechten of de samenleving als geheel, en dat op grote schaal in de hele waardeketen kan worden verspreid;

- 66) “AI-systeem voor algemene doeleinden”: een AI-systeem dat is gebaseerd op een AI-model voor algemene doeleinden en dat verschillende doeleinden kan dienen, zowel voor direct gebruik als voor integratie in andere AI-systemen;
- 67) “zwevendekomma bewerking of “floating-point operation (FLOP)”: elke wiskundige bewerking of toewijzing met zwevendekommagetallen, die een subset vormen van de reële getallen die gewoonlijk op computers worden gerepresenteerd door een geheel getal met een vaste precisie, geschaald door een gehele exponent van een vaste basis;
- 68) “aanbieder verder in de AI-waardeketen”: een aanbieder van een AI-systeem, met inbegrip van een AI-systeem voor algemene doeleinden, waarin een AI-model is geïntegreerd, ongeacht of het AI-model door hemzelf wordt verstrekt en verticaal geïntegreerd is of door een andere entiteit wordt aangeboden op basis van contractuele betrekkingen.

Artikel 4

AI-geletterdheid

Aanbieders en gebruiksverantwoordelijken van AI-systemen nemen maatregelen om, zoveel als mogelijk, te zorgen voor een toereikend niveau van AI-geletterdheid bij hun personeel en andere personen die namens hen AI-systemen exploiteren en gebruiken, en houden daarbij rekening met hun technische kennis, ervaring, onderwijs en opleiding en de context waarin de AI-systemen zullen worden gebruikt, evenals met de personen of groepen personen ten aanzien van wie de AI-systemen zullen worden gebruikt.

Hoofdstuk II

Verboden AI-praktijken

Artikel 5

Verboden AI-praktijken

1. De volgende AI-praktijken zijn verboden:
 - a) het in de handel brengen, het in gebruik stellen of het gebruiken van een AI-systeem dat subliminale technieken waarvan personen zich niet bewust zijn of doelbewust manipulatieve of misleidende technieken gebruikt, met als doel of effect het gedrag van personen of een groep personen wezenlijk te verstoren door hun vermogen om een geïnformeerd besluit te nemen merkbaar te belemmeren, waardoor zij een besluit nemen dat zij anders niet hadden genomen, op een wijze die ertoe leidt of er redelijkerwijs waarschijnlijk toe zal leiden dat deze of andere personen, of een groep personen, aanzienlijke schade oplopen;
 - b) het in de handel brengen, het in gebruik stellen of het gebruiken van een AI-systeem dat gebruikmaakt van de kwetsbaarheden van een natuurlijke persoon of specifieke groep personen als gevolg van hun leeftijd, handicap of een specifieke sociale of economische omstandigheid, met als doel of met als gevolg het gedrag van die persoon of personen die tot deze groep behoren, wezenlijk te verstoren op een wijze die ertoe leidt of waarvan redelijkerwijze te verwachten is dat deze ertoe zal leiden dat deze of andere personen aanzienlijke schade oplopen;

- c) het in de handel brengen, het in gebruik stellen of het gebruiken van AI-systemen voor de evaluatie of classificatie van natuurlijke personen of groepen personen gedurende een bepaalde periode op basis van hun sociale gedrag of bekende, afgeleide of voorspelde persoonlijke of persoonlijkheidskenmerken, waarbij de sociale score een of beide van de volgende gevolgen heeft:
 - i) de nadelige of ongunstige behandeling van bepaalde natuurlijke personen of groepen personen in een sociale context die geen verband houdt met de context waarin de data oorspronkelijk werden gegenereerd of verzameld;
 - ii) de nadelige of ongunstige behandeling van bepaalde natuurlijke personen of groepen personen die ongerechtvaardigd of onevenredig met hun sociale gedrag of de ernst hiervan is;
- d) het in de handel brengen, het voor dit specifieke doel in gebruik stellen of het gebruiken van een AI-systeem voor risicobeoordelingen van natuurlijke personen om het risico dat een natuurlijke persoon een strafbaar feit pleegt te beoordelen of te voorspellen, uitsluitend op basis van de profilering van een natuurlijke persoon of op basis van de beoordeling van diens persoonlijkheidseigenschappen en -kenmerken; dit verbod geldt niet voor AI-systemen die worden gebruikt ter ondersteuning van de menselijke beoordeling van de betrokkenheid van een persoon bij een criminele activiteit, die reeds op rechtstreeks met de criminele activiteit verband houdende objectieve en verifieerbare feiten is gebaseerd;
- e) het in de handel brengen, het voor dit specifieke doel in gebruik stellen of het gebruiken van AI-systemen die databanken voor gezichtsherkenning aanleggen of aanvullen door ongerichte scraping van gezichtsafbeeldingen van internet of CCTV-beelden;

- f) het in de handel brengen, het voor dit specifieke doel in gebruik stellen of het gebruiken van AI-systemen om emoties van een natuurlijke persoon op de werkplek en in het onderwijs uit af te leiden, behalve wanneer het gebruik van het AI-systeem is bedoeld om uit medische of veiligheidsoverwegingen te worden ingevoerd of in de handel te worden gebracht;
- g) het in de handel brengen, het voor dit specifieke doel in gebruik stellen of het gebruiken van systemen voor biometrische categorisering die natuurlijke personen individueel in categorieën indelen op basis van biometrische gegevens om hun ras, politieke opvattingen, lidmaatschap van een vakbond, religieuze of levensbeschouwelijke overtuigingen, seksleven of seksuele gerichtheid af te leiden; dit verbod geldt niet voor het labelen of filteren van rechtmatig verkregen biometrische datasets, zoals afbeeldingen, op basis van biometrische gegevens of categorisering van biometrische gegevens op het gebied van rechtshandhaving;
- h) het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving, tenzij en voor zover een dergelijk gebruik strikt noodzakelijk is voor een van de volgende doelstellingen:
 - i) het gericht zoeken naar specifieke slachtoffers van ontvoering, mensenhandel of seksuele uitbuiting van mensen, alsook het zoeken naar vermiste personen;
 - ii) het voorkomen van een specifieke, aanzienlijke en imminente dreiging voor het leven of de fysieke veiligheid van natuurlijke personen of een reële en actuele of reële en voorspelbare dreiging van een terroristische aanslag;

- iii) de lokalisatie of identificatie van een persoon die ervan wordt verdacht een strafbaar feit te hebben gepleegd, ten behoeve van een strafrechtelijk onderzoek of vervolging of tenuitvoerlegging van een straf voor in bijlage II genoemde strafbare feiten waarop in de betrokken lidstaat een vrijheidsstraf of een tot vrijheidsbeneming strekkende maatregel staat met een maximumduur van ten minste vier jaar.

Punt h) van de eerste alinea doet geen afbreuk aan artikel 9 van Verordening (EU) 2016/679 voor de verwerking van biometrische gegevens voor andere doeleinden dan rechtshandhaving.

- 2. Het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving voor de in lid 1, eerste alinea, punt h), bedoelde doelstellingen wordt ingezet voor de in dat punt bedoelde doeleinden, uitsluitend om de identiteit van de specifiek beoogde persoon te bevestigen en daarbij wordt rekening gehouden met het volgende:
 - a) de aard van de situatie die aanleiding geeft tot het mogelijke gebruik van het systeem, met inbegrip van de ernst, waarschijnlijkheid en omvang van de schade die zonder het gebruik van het systeem zou worden veroorzaakt;
 - b) de gevolgen van het gebruik van het systeem voor de rechten en vrijheden van alle betrokken personen, en met name de ernst, waarschijnlijkheid en omvang van deze gevolgen.

Daarnaast moet het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving voor de in lid 1, eerste alinea, punt h), genoemde doelstellingen in overeenstemming zijn met noodzakelijke en evenredige waarborgen en voorwaarden in verband met het gebruik in overeenstemming met het nationale recht dat het gebruik ervan toelaat, en met name ten aanzien van de beperking in de tijd en de geografische en persoonlijke beperkingen. Het gebruik van het systeem voor biometrische identificatie op afstand in real time in openbare ruimten wordt alleen toegestaan indien de rechtshandhavingsinstantie een in artikel 27 voorziene effectbeoordeling op het gebied van de grondrechten heeft uitgevoerd en het systeem volgens artikel 49 in de EU-databank heeft geregistreerd. In naar behoren gemotiveerde spoedeisende gevallen kan echter met het gebruik van dergelijke systemen worden begonnen zonder de systemen in de EU-databank te registreren, op voorwaarde dat die registratie zonder onnodige vertraging wordt voltooid.

3. Voor de toepassing van lid 1, eerste alinea, punt h), en lid 2, wordt elk gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving afhankelijk gesteld van een voorafgaande toestemming die wordt verleend door een gerechtelijke instantie of een onafhankelijke administratieve instantie, waarvan het besluit bindend is, van de lidstaat waarin het gebruik moet plaatsvinden en die wordt gegeven op verzoek en in overeenstemming met de gedetailleerde regels van het nationale recht als bedoeld in lid 5. In een naar behoren gemotiveerde spoedeisende situatie kan echter zonder toestemming met het gebruik van een dergelijk systeem worden begonnen, op voorwaarde dat een dergelijke toestemming zonder onnodige vertraging en ten minste binnen 24 uur wordt aangevraagd. Bij weigering van die toestemming wordt het gebruik onmiddellijk gestaakt en worden alle gegevens, resultaten en outputs van dat gebruik onmiddellijk verwijderd en gewist.

De bevoegde gerechtelijke instantie of onafhankelijke administratieve instantie, waarvan het besluit bindend is verleent de toestemming slechts wanneer zij op basis van objectief bewijs of duidelijke indicaties die aan haar zijn voorgelegd ervan overtuigd is dat het gebruik van het betreffende systeem voor biometrische identificatie op afstand in real time noodzakelijk is voor en evenredig is aan het bereiken van een van de in lid 1, eerste alinea, punt h), gespecificeerde doelstellingen, zoals genoemd in het verzoek en met name beperkt blijft tot wat strikt noodzakelijk is met betrekking tot de periode en de geografische en personele werkingssfeer. Bij haar beslissing over het verzoek houdt die instantie rekening met de in lid 2 bedoelde elementen. Een besluit dat nadelige rechtsgevolgen heeft voor een persoon mag niet uitsluitend worden genomen op basis van de output van het systeem voor biometrische identificatie op afstand in real time.

4. Onverminderd lid 3 wordt elk gebruik van een systeem voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving gemeld bij de bevoegde markttoezichtautoriteit en de nationale gegevensbeschermingsautoriteit in overeenstemming met de in lid 5 bedoelde nationale regels. Die melding bevat ten minste de in lid 6 bepaalde informatie en bevat geen gevoelige operationele gegevens.

5. Een lidstaat kan besluiten om te voorzien in de mogelijkheid om volledig of gedeeltelijk toestemming te verlenen voor het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving binnen de grenzen en onder de voorwaarden van lid 1, eerste alinea, punt h), en de leden 2 en 3. De betrokken lidstaten leggen in hun nationale recht de noodzakelijke gedetailleerde regels vast voor het verzoek om en de afgifte en het gebruik van, evenals het toezicht en verslaglegging in verband met, de in lid 3 bedoelde vergunningen. In deze regels wordt ook gespecificeerd voor welke doelstellingen van lid 1, eerste alinea, punt h), en voor welke strafbare feiten als bedoeld in punt h), iii), daarvan de bevoegde autoriteiten deze systemen mogen gebruiken met het oog op de rechtshandhaving. De lidstaten stellen de Commissie uiterlijk 30 dagen na de vaststelling van die regels in kennis. De lidstaten kunnen in overeenstemming met het Unierecht restrictievere wetgeving inzake het gebruik van systemen voor biometrische identificatie op afstand invoeren.
6. Nationale markttoezichtautoriteiten en nationale gegevensbeschermingsautoriteiten van lidstaten die op grond van lid 4 in kennis zijn gesteld van het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving, dienen bij de Commissie jaarverslagen over dat gebruik in. Daartoe verstrekt de Commissie de lidstaten en de nationale markttoezicht- en gegevensbeschermingsautoriteiten een sjabloon, met informatie over het aantal besluiten dat is genomen door bevoegde gerechtelijke instanties of een onafhankelijke administratieve instantie, waarvan het besluit bindend is overeenkomstig lid 3, alsook het resultaat van die besluiten.

7. De Commissie publiceert jaarverslagen over het gebruik van systemen voor biometrische identificatie op afstand in real time in openbare ruimten met het oog op de rechtshandhaving, op basis van geaggregeerde gegevens in de lidstaten op basis van de in lid 6 bedoelde jaarverslagen. Die jaarverslagen bevatten geen gevoelige operationele gegevens van de gerelateerde rechtshandhavingsactiviteiten.
8. Dit artikel doet geen afbreuk aan de verbodsbepalingen die van toepassing zijn wanneer een AI-praktijk een inbreuk vormt op het Unierecht.

Hoofdstuk III

AI-systemen met een hoog risico

AFDELING 1

CLASSIFICATIE VAN AI-SYSTEMEN ALS AI-SYSTEMEN MET EEN HOOG RISICO

Artikel 6

Classificatieregels voor AI-systemen met een hoog risico

1. Ongeacht of een AI-systeem los van in de punten a) en b) bedoelde producten in de handel wordt gebracht of in gebruik wordt gesteld, wordt een AI-systeem als AI-systeem met een hoog risico beschouwd wanneer aan beide van de volgende voorwaarden is voldaan:
 - a) het AI-systeem is bedoeld om te worden gebruikt als veiligheidscomponent van een product of het AI-systeem is zelf een product dat valt onder de in bijlage I opgenomen harmonisatiewetgeving van de Unie;

- b) voor het product waarvan het AI-systeem de veiligheidscomponent op grond van punt a) vormt of voor het AI-systeem als product zelf moet een conformiteitsbeoordeling door een derde partij worden uitgevoerd met het oog op het in de handel brengen of in gebruik stellen van dat product op grond van de in bijlage I opgenomen harmonisatiewetgeving van de Unie.
2. Naast de in lid 1 bedoelde AI-systemen met een hoog risico worden ook AI-systemen zoals bedoeld in bijlage III als AI-systeem met een hoog risico beschouwd.
3. In afwijking van lid 2 wordt een in bijlage III bedoeld AI-systeem niet als AI-systeem met een hoog risico beschouwd wanneer het geen significant risico op schade voor de gezondheid, veiligheid of de grondrechten van natuurlijke personen inhoudt, onder meer doordat het de uitkomst van de besluitvorming niet wezenlijk beïnvloedt.

De eerste alinea is van toepassing wanneer aan een van de volgende voorwaarden is voldaan:

- a) het AI-systeem is bedoeld om een beperkte procedurele taak uit te voeren;
- b) het AI-systeem is bedoeld om het resultaat van een eerder voltooide menselijke activiteit te verbeteren;
- c) het AI-systeem is bedoeld om besluitvormingspatronen of afwijkingen van eerdere besluitvormingspatronen op te sporen en is niet bedoeld om de eerder voltooide menselijke beoordeling zonder behoorlijke menselijke toetsing te vervangen of te beïnvloeden; of
- d) het AI-systeem is bedoeld om een voorbereidende taak uit te voeren voor een beoordeling die relevant is voor de in bijlage III vermelde gebruikgevallen.

Niettegenstaande de eerste alinea wordt een in bijlage III bedoeld AI-systeem altijd als een AI-systeem met een hoog risico beschouwd indien het AI-systeem profilering van natuurlijke personen uitvoert.

4. Een aanbieder die van mening is dat een in bijlage III bedoeld AI-systeem geen hoog risico inhoudt, documenteert zijn beoordeling voordat dat systeem in de handel wordt gebracht of in gebruik wordt gesteld. Die aanbieder is onderworpen aan de registratieverplichting van artikel 49, lid 2. Op verzoek van de nationale bevoegde autoriteiten verstrekt de aanbieder de documentatie van de beoordeling.
5. De Commissie verstrekt na raadpleging van de Europese raad voor artificiële intelligentie (de “AI-board”) en uiterlijk op ... [18 maanden na de datum van inwerkingtreding van deze verordening] richtsnoeren voor de praktische uitvoering van dit artikel in overeenstemming met artikel 96, samen met een uitgebreide lijst van praktische voorbeelden van gebruikgevallen van AI-systemen met een hoog risico en zonder hoog risico.
6. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen om teneinde lid 3, tweede alinea, van dit artikel te wijzigen door nieuwe voorwaarden toe te voegen aan de daarin vastgelegde voorwaarden, of door hen te wijzigen, indien er concrete en betrouwbare bewijzen zijn voor het bestaan van AI-systemen die onder het toepassingsgebied van bijlage III vallen, maar die geen significant risico inhouden op schade voor de gezondheid, veiligheid of grondrechten van natuurlijke personen.

7. De Commissie stelt overeenkomstig artikel 97 gedelegeerde handelingen vast om lid 3, tweede alinea, van dit artikel te wijzigen door de daarin vastgelegde voorwaarden te schrappen, indien er concrete en betrouwbare aanwijzingen zijn dat dit noodzakelijk is om het in deze verordening bepaalde niveau van bescherming van de gezondheid, de veiligheid en de grondrechten te behouden.
8. Overeenkomstig de leden 6 en 7 van dit artikel vastgestelde wijzigingen van de in lid 3, tweede alinea, vastgelegde voorwaarden doen geen afbreuk aan het in deze verordening bepaalde algemene niveau van bescherming van de gezondheid, de veiligheid en de grondrechten, en zorgen voor samenhang met de op grond van artikel 7, lid 1, vastgestelde gedelegeerde handelingen en houden rekening met markt- en technologische ontwikkelingen.

Artikel 7

Wijzigingen in bijlage III

1. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen tot wijziging van bijlage III door hieraan gebruiksgevallen van AI-systemen met een hoog risico toe te voegen of te wijzigen wanneer aan beide van de volgende voorwaarden is voldaan:
 - a) de AI-systemen zijn bedoeld om te worden gebruikt op een van de gebieden als bedoeld in bijlage III;
 - b) de AI-systemen vormen een risico op schade voor de gezondheid en veiligheid, of nadelige effecten op de grondrechten, en dat risico is gelijk aan of groter dan het risico op schade of nadelige effecten dat wordt gevormd door de AI-systemen met een hoog risico die reeds zijn opgenomen in bijlage III.

2. Bij de beoordeling van de voorwaarde van lid 1, punt b), houdt de Commissie rekening met de volgende criteria:
- a) het beoogde doel van het AI-systeem;
 - b) de mate waarin een AI-systeem is gebruikt of waarschijnlijk zal worden gebruikt;
 - c) de aard van en de hoeveelheid gegevens die het AI-systeem verwerkt en gebruikt, met name of bijzondere categorieën persoonsgegevens worden verwerkt;
 - d) de mate waarin het AI-systeem autonoom handelt en de mogelijkheid voor een mens om beslissingen of aanbevelingen die tot schade kunnen leiden terzijde te schuiven;
 - e) de mate waarin het gebruik van een AI-systeem reeds schade voor de gezondheid en veiligheid of nadelige effecten op de grondrechten heeft veroorzaakt of aanleiding heeft gegeven tot aanzienlijke zorgen in verband met de waarschijnlijkheid van dergelijke schade of nadelige effecten, zoals aangetoond bijvoorbeeld door verslagen of gedocumenteerde beweringen die zijn ingediend bij de nationale bevoegde autoriteiten of, in voorkomend geval, door andere verslagen;
 - f) de potentiële omvang van dergelijke schade of dergelijke nadelige effecten, met name wat betreft de intensiteit ervan en de mogelijkheid dat meerdere personen worden getroffen of dat een bepaalde groep personen onevenredig wordt getroffen;
 - g) de mate waarin potentieel geschade of nadelig getroffen personen afhankelijk zijn van de aan de hand van een AI-systeem geproduceerde uitkomst, met name omdat het om praktische of juridische redenen niet redelijkerwijs mogelijk is om van deze uitkomst af te zien;

- h) de mate waarin sprake is van een onevenwichtige machtsverhouding, of de potentieel geschade of nadelig getroffen personen zich in een kwetsbare positie bevinden ten opzichte van de gebruiksverantwoordelijke van een AI-systeem, met name als gevolg van status, autoriteit, kennis, economische of sociale omstandigheden of leeftijd;
- i) de mate waarin de geproduceerde uitkomst waarbij een AI-systeem betrokken is niet gemakkelijk kan worden rechtgezet of omgekeerd, rekening houdend met de beschikbare technische oplossingen om die uitkomst recht te zetten of om te keren, waarbij van uitkomsten die nadelige effecten hebben op de gezondheid, veiligheid of grondrechten, niet wordt beschouwd dat zij eenvoudig kunnen worden rechtgezet of omgekeerd;
- j) de omvang en waarschijnlijkheid van het voordeel dat het inzetten van het AI-systeem voor natuurlijke personen, groepen of de samenleving in het algemeen, met inbegrip van mogelijke verbeteringen op het gebied van productveiligheid, met zich meebrengt;
- k) de mate waarin in het bestaande Unierecht is voorzien in:
 - i) doeltreffende maatregelen om beroep aan te tekenen in verband met de risico's van een AI-systeem, met uitzondering van vorderingen tot schadevergoeding;
 - ii) doeltreffende maatregelen om deze risico's te voorkomen of aanzienlijk te beperken.

3. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen tot wijziging van bijlage III door AI-systemen met een hoog risico te schrappen wanneer aan beide van de volgende voorwaarden is voldaan:
- a) het betrokken AI-systeem met een hoog risico vormt, rekening houdend met de in lid 2 vermelde criteria, geen significant risico voor de grondrechten, de gezondheid of de veiligheid;
 - b) de schrapping leidt niet tot een lager algeheel beschermingsniveau wat betreft de gezondheid, de veiligheid en de grondrechten uit hoofde van het Unierecht.

AFDELING 2

EISEN VOOR AI-SYSTEMEN MET EEN HOOG RISICO

Artikel 8

Naleving van de eisen

1. AI-systemen met een hoog risico moeten voldoen aan de eisen van deze afdeling, rekening houdend met hun beoogde doel en de algemeen erkende stand van de techniek op het gebied van AI en AI-gerelateerde technologieën. Bij het waarborgen van de naleving van deze eisen wordt rekening gehouden met het in artikel 9 bedoelde systeem voor risicobeheer.

2. Indien een product een AI-systeem omvat waarop zowel de vereisten van deze verordening als die van de in bijlage I, afdeling A, vermelde harmonisatiewetgeving van de Unie van toepassing zijn, zijn aanbieders ervoor verantwoordelijk te waarborgen dat hun product volledig voldoet aan alle toepasselijke vereisten uit hoofde van de toepasselijke harmonisatiewetgeving van de Unie. Om te waarborgen dat de in lid 1 bedoelde AI-systemen met een hoog risico voldoen aan de eisen van deze afdeling en om te zorgen voor consistentie, dubbel werk te voorkomen en de extra lasten tot een minimum te beperken, hebben aanbieders de keuze om in voorkomend geval de nodige test- en rapportageprocessen en door hen verstrekte informatie en documentatie over hun product op te nemen in de reeds bestaande documentatie en procedures die vereist zijn uit hoofde van de in bijlage I, afdeling A, bedoelde harmonisatiewetgeving van de Unie.

Artikel 9

Systeem voor risicobeheer

1. Met betrekking tot AI-systemen met een hoog risico wordt een systeem voor risicobeheer vastgesteld, uitgevoerd, gedocumenteerd en in stand gehouden.
2. Onder het systeem voor risicobeheer wordt verstaan een tijdens de gehele levensduur van een AI-systeem met een hoog risico doorlopend en gepland iteratief proces, dat periodieke systematische toetsing en actualisering vereist. Het omvat de volgende stappen:
 - a) het vaststellen en analyseren van de bekende en de redelijkerwijs te voorziene risico's die het AI-systeem met een hoog risico kan inhouden voor de gezondheid, veiligheid of grondrechten indien het AI-systeem met een hoog risico in overeenstemming met het beoogde doel ervan wordt gebruikt;

- b) het inschatten en evalueren van de risico's die zich kunnen voordoen wanneer het AI-systeem met een hoog risico wordt gebruikt in overeenstemming met het beoogde doel ervan en in een situatie van redelijkerwijs te voorzien misbruik;
 - c) het evalueren van andere risico's die zich kunnen voordoen op basis van de analyse van de data die zijn verzameld door het systeem voor monitoring na het in de handel brengen, als bedoeld in artikel 72;
 - d) het vaststellen van gepaste en gerichte risicobeheersmaatregelen om de op grond van punt a) vastgestelde risico's aan te pakken.
3. De in dit artikel bedoelde risico's omvatten uitsluitend risico's die redelijkerwijs kunnen worden beperkt of weggenomen via het ontwikkelen of ontwerpen van het AI-systeem met een hoog risico of de verstrekking van adequate technische informatie.
4. Ten aanzien van de in lid 2, punt d), bedoelde risicobeheersmaatregelen wordt naar behoren rekening gehouden met de effecten en mogelijke wisselwerking die voortvloeien uit de gecombineerde toepassing van de in deze afdeling uiteengezette eisen, teneinde de risico's doeltreffender tot een minimum te beperken en tegelijkertijd een passend evenwicht te bereiken bij de uitvoering van de maatregelen ter vervulling van de voorschriften.
5. De in lid 2, punt d), bedoelde risicobeheersmaatregelen zijn zodanig dat het desbetreffende restrisico in verband met elk gevaar en het totale restrisico van de AI-systemen met een hoog risico aanvaardbaar wordt geacht.

Bij het vaststellen van de passendste risicobeheersmaatregelen wordt het volgende gewaarborgd:

- a) uitsluiting of beperking van op grond van lid 2 vastgestelde en geëvalueerde risico's voor zover technisch haalbaar door middel van een adequaat ontwerp en ontwikkeling van het AI-systeem met een hoog risico;
- b) waar passend worden adequate maatregelen voor beperking en controle genomen voor het aanpakken van risico's die niet kunnen worden uitgesloten;
- c) verstrekking van op grond van artikel 13 vereiste informatie en waar passend opleiding voor gebruiksverantwoordelijken.

Teneinde de risico's in verband met het gebruik van het AI-systeem met een hoog risico weg te nemen of te beperken, wordt naar behoren aandacht besteed aan de te verwachten technische kennis, ervaring, scholing en opleiding van de gebruiksverantwoordelijke en de vermoedelijke context waarin het systeem dient te worden gebruikt.

- 6. AI-systemen met een hoog risico worden getest met het oog op het vaststellen van de passendste en gerichte risicobeheersmaatregelen. De tests zorgen ervoor dat AI-systemen met een hoog risico consistent presteren ten aanzien van het beoogde doel ervan en in overeenstemming zijn met de eisen van deze afdeling.
- 7. De testprocedures kunnen onder meer bestaan in testen onder reële omstandigheden overeenkomstig artikel 60.

8. Het testen van AI-systemen met een hoog risico vindt, zoals passend, in de loop van het ontwikkelingsproces plaats en in ieder geval voordat het systeem in de handel wordt gebracht of in gebruik wordt gesteld. Er wordt getest aan de hand van vooraf vastgestelde beoordelingsmaatstaven en probabilistische drempels die passend zijn voor het beoogde doel van het AI-systeem met een hoog risico.
9. Bij de uitvoering van het in de leden 1 tot en met 7 bepaalde systeem voor risicobeheer houden aanbieders rekening met de vraag of het beoogde doel van het AI-systeem met een hoog risico waarschijnlijk negatieve gevolgen zal hebben voor personen jonger dan 18 jaar en, in voorkomend geval, voor andere kwetsbare groepen.
10. Voor aanbieders van AI-systemen met een hoog risico die onderworpen zijn aan eisen met betrekking tot interne risicobeheerprocessen uit hoofde van andere relevante bepalingen van het Unierecht, kunnen de in de leden 1 tot en met 9 bepaalde aspecten deel uitmaken van of gecombineerd worden met de op grond van dat recht vastgestelde risicobeheerprocedures.

Artikel 10

Data en datagovernance

1. AI-systemen met een hoog risico die technieken gebruiken die het trainen van AI-modellen met data omvatten, worden ontwikkeld op basis van datasets voor training, validatie en tests die voldoen aan de in de leden 2 tot en met 5 bedoelde kwaliteitscriteria telkens wanneer dergelijke datasets worden gebruikt.

2. Datasets voor training, validatie en tests worden onderworpen aan praktijken op het gebied van databeheer die stroken met het beoogde doel van het AI-systeem met een hoog risico. Deze praktijken hebben in het bijzonder betrekking op:
- a) de relevante ontwerpkeuzes;
 - b) processen voor dataverzameling en de oorsprong van de data en, in het geval van persoonsgegevens, het oorspronkelijke doel van de dataverzameling;
 - c) relevante verwerkingsactiviteiten voor datavoorbereiding, zoals annotatie, labelen, opschoning, actualisatie, verrijking en aggregatie;
 - d) het opstellen van aannames, met name met betrekking tot de informatie die de data moeten meten en vertegenwoordigen;
 - e) een beoordeling van de beschikbaarheid, kwantiteit en geschiktheid van de datasets die nodig zijn;
 - f) een beoordeling met het oog op mogelijke vooringenomenheid die waarschijnlijk gevolgen heeft voor de gezondheid en de veiligheid van personen, nadelige effecten heeft op de grondrechten, of leidt tot discriminatie die op grond van het Unierecht verboden is, vooral wanneer data-outputs invloed hebben op inputs voor toekomstige operaties;
 - g) en passende maatregelen om mogelijke overeenkomstig punt f) vastgestelde vertekeningen op te sporen, te voorkomen en te beperken;
 - h) het identificeren van relevante leemten of tekortkomingen in de data die naleving van deze verordening in de weg staan, en de manier waarop deze leemten en tekortkomingen kunnen worden aangepakt.

3. Datasets voor training, validatie en tests zijn relevant, voldoende representatief, en zoveel mogelijk foutenvrij en volledig met het oog op het beoogde doel. De datasets hebben bovendien de passende statistische kenmerken, onder meer, waar van toepassing, met betrekking tot de personen of groepen personen ten aanzien van wie de AI-systemen met een hoog risico moeten worden gebruikt. Deze kenmerken van de datasets kunnen op het niveau van de afzonderlijke datasets of combinatie daarvan worden verwezenlijkt.
4. Ten aanzien van datasets wordt, voor zover vereist gezien het beoogde doel hiervan, rekening gehouden met de eigenschappen of elementen die specifiek zijn voor een bepaalde geografische, contextuele, functionele of gedragsomgeving waarin het AI-systeem met een hoog risico moet worden gebruikt.
5. Voor zover dit strikt noodzakelijk is om de opsporing en correctie van vertekeningen te waarborgen in verband met de AI-systemen met een hoog risico overeenkomstig lid 2, punten f) en g), van dit artikel, mogen de aanbieders van dergelijke systemen uitzonderlijk bijzondere categorieën persoonsgegevens verwerken, mits passende waarborgen worden geboden voor de grondrechten en fundamentele vrijheden van natuurlijke personen. Naast de bepalingen van Verordeningen (EU) 2016/679 en (EU) 2018/1725 en Richtlijn (EU) 2016/680 moeten voor een dergelijke verwerking alle volgende voorwaarden van toepassing zijn vervuld:
 - a) de opsporing en correctie van vooringenomenheid kunnen niet doeltreffend worden vervuld door het verwerken van andere data, waaronder synthetische of geanonimiseerde data;

- b) de bijzondere categorieën persoonsgegevens zijn onderworpen aan technische beperkingen voor het hergebruik van persoonsgegevens, en geavanceerde beveiligings- en privacybeschermingsmaatregelen, waaronder pseudonimisering;
- c) de bijzondere categorieën persoonsgegevens zijn onderworpen aan maatregelen om ervoor te zorgen dat de verwerkte persoonsgegevens worden beveiligd, beschermd met passende waarborgen, waaronder strikte controles en documentatie van de toegang ertoe, om misbruik te voorkomen en ervoor te zorgen dat alleen personen die gemachtigd zijn toegang tot die persoonsgegevens hebben met passende vertrouwelijkheidsverplichtingen;
- d) de bijzondere categorieën persoonsgegevens worden niet verzonden, doorgegeven of anderszins geraadpleegd door andere partijen;
- e) de bijzondere categorieën persoonsgegevens worden verwijderd zodra de vertekening is gecorrigeerd of de periode van bewaring van de persoonsgegevens ten einde is gekomen, indien dit eerder is;
- f) het register op grond van Verordeningen (EU) 2016/679 en (EU) 2018/1725 en Richtlijn (EU) 2016/680 van verwerkingsactiviteiten bevat de redenen waarom de verwerking van bijzondere categorieën persoonsgegevens strikt noodzakelijk was om vertekeningen op te sporen en waarom die doelstelling niet kon worden bereikt door de verwerking van andere data.

6. Voor de ontwikkeling van AI-systemen met een hoog risico die geen technieken voor de training van modellen gebruiken, zijn de leden 2 tot en met 5 uitsluitend van toepassing op de datasets voor tests.

Artikel 11
Technische documentatie

1. De technische documentatie van een AI-systeem met een hoog risico wordt opgesteld voordat dit systeem in de handel wordt gebracht of in gebruik wordt gesteld, en wordt geactualiseerd.

De technische documentatie wordt op zodanige wijze opgesteld dat wordt aangetoond dat het AI-systeem met een hoog risico in overeenstemming is met de eisen van deze afdeling en dat nationale bevoegde autoriteiten en aangemelde instanties over de noodzakelijke, op heldere en begrijpelijke wijze gestelde informatie beschikken om de overeenstemming van het AI-systeem met deze voorschriften te kunnen beoordelen. De documentatie omvat ten minste de in bijlage IV uiteengezette elementen. Kmo's, met inbegrip van start-ups, kunnen de elementen van de in bijlage IV gespecificeerde technische documentatie op vereenvoudigde wijze verstrekken. Daartoe stelt de Commissie een vereenvoudigd formulier voor technische documentatie op dat is afgestemd op de behoeften van kleine en micro-ondernemingen. Kmo's, met inbegrip van start-ups, die ervoor kiezen de in bijlage IV vereiste informatie op vereenvoudigde wijze te verstrekken, gebruiken het in dit lid bedoelde formulier. Aangemelde instanties aanvaarden het formulier met het oog op de conformiteitsbeoordeling.

2. Wanneer een AI-systeem met een hoog risico dat verband houdt met een product dat valt onder de in bijlage I, afdeling A, opgenomen harmonisatiewetgeving van de Unie in de handel wordt gebracht of in gebruik wordt gesteld, wordt een enkel technisch document opgesteld dat alle informatie bevat zoals uiteengezet in lid 1, alsook de informatie die vereist is op grond van die rechtshandelingen.

3. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen om, waar nodig, bijlage IV te wijzigen om, in het licht van de technische vooruitgang, te waarborgen dat in de technische documentatie alle noodzakelijke informatie wordt verstrekt om de overeenstemming van het systeem met de eisen van deze afdeling te kunnen beoordelen.

Artikel 12

Registratie

1. AI-systemen met een hoog risico zijn dusdanig technisch vormgegeven dat gebeurtenissen gedurende de levenscyclus van het systeem automatisch worden geregistreerd (“logs”).
2. Teneinde ervoor te zorgen dat de werking van het AI-systeem met een hoog risico een niveau van traceerbaarheid heeft dat passend is voor het beoogde doel van het systeem, maken loggingfuncties het mogelijk om gebeurtenissen te registreren die relevant zijn ter:
 - a) identificatie van situaties die ertoe kunnen leiden dat het AI-systeem met een hoog risico een risico vormt in de zin van artikel 79, lid 1, of dat er een substantiële wijziging optreedt;
 - b) facilitering van de in artikel 72 bedoelde monitoring na het in de handel brengen; en
 - c) monitoring van de werking van in artikel 26, lid 5, bedoelde AI-systemen met een hoog risico.
3. Voor AI-systemen met een hoog risico als bedoeld in punt 1, a), van bijlage III voorzien de loggingcapaciteiten ten minste in:
 - a) de registratie van de duur van elk gebruik van het systeem (begindatum en -tijd en einddatum en -tijd van elk gebruik);

- b) de referentiedatabank aan de hand waarvan de inputdata zijn gecontroleerd door het systeem;
- c) de inputdata ten aanzien waarvan de zoekopdracht een match heeft opgeleverd;
- d) de identificatie van de natuurlijke personen die betrokken zijn bij de verificatie van de resultaten, zoals bedoeld in artikel 14, lid 5.

Artikel 13

Transparantie en informatieverstrekking aan gebruiksverantwoordelijken

1. AI-systemen met een hoog risico worden op zodanige wijze ontworpen en ontwikkeld dat de werking ervan voldoende transparant is om gebruiksverantwoordelijken in staat te stellen de output van een systeem te interpreteren en op passende wijze te gebruiken. Een passende soort en mate van transparantie wordt gewaarborgd met het oog op de naleving van de relevante verplichtingen van de aanbieder en de gebruiksverantwoordelijke zoals uiteengezet in afdeling 3.
2. AI-systemen met een hoog risico gaan vergezeld van gebruiksinstructies in een passend digitaal of ander formaat dat beknopte, volledige, juiste en duidelijke informatie bevat die relevant, toegankelijk en begrijpelijk is voor gebruiksverantwoordelijken.
3. De gebruiksinstructies bevatten ten minste de volgende gegevens:
 - a) de identiteit en de contactgegevens van de aanbieder en, in voorkomend geval, van zijn gemachtigde;

- b) de kenmerken, capaciteiten en beperkingen van de prestaties van het AI-systeem met een hoog risico, waaronder:
- i) het beoogde doel;
 - ii) de mate van nauwkeurigheid, waaronder de beoordelingsmaatstaven, robuustheid en cyberbeveiliging als bedoeld in artikel 15 waarop het AI-systeem met een hoog risico is getest en gevalideerd en die kan worden verwacht, en eventuele bekende en te voorziene omstandigheden die een effect kunnen hebben op die verwachte mate van nauwkeurigheid, robuustheid en cyberbeveiliging;
 - iii) eventuele bekende of te voorziene omstandigheden in verband met het gebruik van het AI-systeem met een hoog risico in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik, die kunnen leiden tot risico's voor de gezondheid en veiligheid of de grondrechten als bedoeld in artikel 9, lid 2;
 - iv) in voorkomend geval, de technische capaciteiten en kenmerken van het AI-systeem met een hoog risico om informatie te verstrekken die relevant is om de output ervan toe te lichten;
 - v) in voorkomend geval, zijn prestaties met betrekking tot specifieke personen of groepen personen voor wie het systeem moet worden gebruikt;
 - vi) in voorkomend geval, specificaties voor de inputdata of eventuele andere relevante informatie met betrekking tot de gebruikte datasets voor training, validatie en tests, rekening houdend met het beoogde doel van het AI-systeem met een hoog risico;

- vii) in voorkomend geval, informatie om de gebruiksverantwoordelijken in staat te stellen de output van het AI-systeem met een hoog risico te interpreteren en op passende wijze te gebruiken;
- c) de wijzigingen van het AI-systeem met een hoog risico en de prestaties ervan die vooraf door de aanbieder zijn bepaald op het moment van de eerste conformiteitsbeoordeling, indien van toepassing;
- d) de in artikel 14 bedoelde maatregelen voor menselijk toezicht, met inbegrip van de technische maatregelen die zijn getroffen om de interpretatie van de output van de AI-systemen met een hoog risico door gebruiksverantwoordelijken te vergemakkelijken;
- e) de benodigde rekenkracht en hardware, de verwachte levensduur van het AI-systeem met een hoog risico en eventuele noodzakelijke maatregelen – en de frequentie daarvan – voor onderhoud en verzorging ter waarborging van de goede werking van dat AI-systeem, ook in verband met software-updates;
- f) in voorkomend geval, een beschrijving van de mechanismen in het AI-systeem met een hoog risico die gebruiksverantwoordelijken in staat stellen de logs naar behoren te verzamelen, op te slaan en te interpreteren overeenkomstig artikel 12.

Artikel 14

Menselijk toezicht

1. AI-systemen met een hoog risico worden zodanig ontworpen en ontwikkeld, met inbegrip van passende mens-machine-interface-instrumenten, dat hierop tijdens de periode dat zij worden gebruikt, op doeltreffende wijze toezicht kan worden uitgeoefend door natuurlijke personen.

2. Het menselijk toezicht is gericht op het voorkomen of beperken van de risico's voor de gezondheid, veiligheid of grondrechten die zich kunnen voordoen wanneer een AI-systeem met een hoog risico wordt gebruikt in overeenstemming met het beoogde doel ervan of in een situatie van redelijkerwijs te voorzien misbruik, met name wanneer dergelijke risico's blijven bestaan ondanks de toepassing van andere eisen van deze afdeling.
3. De toezichtmaatregelen staan in verhouding met de risico's, de mate van autonomie en de gebruikscontext van het AI-systeem met een hoog risico en worden gewaarborgd door middel van een of alle van de volgende soorten maatregelen:
 - a) door de aanbieder bepaalde maatregelen die waar technisch haalbaar in het AI-systeem met een hoog risico worden ingebouwd voordat dit systeem in de handel wordt gebracht of in gebruik wordt gesteld;
 - b) door de aanbieder bepaalde maatregelen voordat het AI-systeem met een hoog risico in de handel wordt gebracht of in gebruik wordt gesteld en die passend zijn om door de gebruiksverantwoordelijke te worden uitgevoerd.
4. Met het oog op de uitvoering van de leden 1, 2 en 3 wordt het AI-systeem met een hoog risico zodanig aan de gebruiksverantwoordelijke verstrekt dat natuurlijke personen die verantwoordelijk zijn voor het menselijk toezicht, in staat worden gesteld om waar passend en evenredig:
 - a) de relevante capaciteiten en beperkingen van het AI-systeem met een hoog risico goed te begrijpen en de werking ervan naar behoren te kunnen monitoren, onder meer met het oog op het opsporen en aanpakken van onregelmatigheden, storingen en onverwachte prestaties;

- b) zich bewust te blijven van de mogelijke neiging om automatisch of te veel te vertrouwen op de output van een AI-systeem met een hoog risico (de zogenaamde “automation bias”), met name voor AI-systemen met een hoog risico die worden gebruikt om informatie of aanbevelingen te verstrekken voor beslissingen die door natuurlijke personen moeten worden genomen;
- c) de output van het AI-systeem met een hoog risico juist te interpreteren, bijvoorbeeld de beschikbare instrumenten en methoden voor interpretatie;
- d) in alle specifieke situaties te kunnen besluiten om het AI-systeem met een hoog risico niet te gebruiken of de output van het AI-systeem met een hoog risico op andere wijze te negeren, door een andere beslissing te vervangen of terug te draaien;
- e) in te grijpen in de werking van het AI-systeem met een hoog risico of het systeem te onderbreken door middel van een stopknop of een vergelijkbare procedure waarmee het systeem op veilige wijze kan worden stopgezet.

5. Voor AI-systemen met een hoog risico als bedoeld in bijlage III, punt 1, a), zijn de maatregelen als bedoeld in lid 3 van dit artikel zodanig dat zij waarborgen dat daarnaast door de gebruiksverantwoordelijke geen maatregelen worden getroffen of beslissingen worden genomen op basis van de identificatie door het systeem, tenzij deze identificatie door ten minste twee natuurlijke personen met de nodige bekwaamheid, opleiding en bevoegdheid apart zijn geverifieerd en bevestigd.

Het vereiste van een afzonderlijke verificatie door ten minste twee natuurlijke personen is niet van toepassing op AI-systemen met een hoog risico die gebruikt worden voor rechtshandhaving, migratie, grenstoezicht of asiel, in gevallen waarin het Unierecht of het nationale recht de toepassing van dit vereiste onevenredig acht.

Artikel 15

Nauwkeurigheid, robuustheid en cyberbeveiliging

1. AI-systemen met een hoog risico worden op zodanige wijze ontworpen en ontwikkeld dat deze een passend niveau van nauwkeurigheid, robuustheid en cyberbeveiliging bieden, alsook consistente prestaties gedurende de levensduur met betrekking tot deze aspecten.
2. Ter verduidelijking van de technische aspecten van de meting van het passende niveau van nauwkeurigheid en robuustheid als bedoeld in lid 1 en andere relevante prestatiestatistieken, moedigt de Commissie, in samenwerking met relevante belanghebbenden en organisaties, zoals metrologie- en benchmarkingautoriteiten, waar passend, de ontwikkeling van benchmarks en meetmethoden aan.
3. De niveaus van nauwkeurigheid en de relevante maatstaven voor de nauwkeurigheid van AI-systemen met een hoog risico worden vermeld in de bijbehorende gebruiksaanwijzingen.
4. AI-systemen met een hoog risico zijn zo goed mogelijk bestand tegen fouten en onregelmatigheden die zich binnen het systeem of de omgeving waarin het systeem wordt gebruikt, kunnen voordoen, met name als gevolg van de interactie ervan met natuurlijke personen of andere systemen. In dat opzicht worden technische en organisatorische maatregelen genomen.

De robuustheid van AI-systemen met een hoog risico kan worden gerealiseerd door middel van technische oplossingen voor redundantie, die plannen voor de back-up of de veiligheid bij defecten kunnen omvatten.

AI-systemen met een hoog risico die blijven leren nadat ze in de handel zijn gebracht of in gebruik zijn gesteld, worden op zodanige wijze ontwikkeld dat het risico op beïnvloeding van toekomstige operaties door gebruik van vertekende outputs als input (“feedback loops”) wordt weggenomen of zo veel mogelijk worden beperkt en dat elke dergelijke feedback loop naar behoren wordt aangepakt met behulp van passende beperkende maatregelen.

5. AI-systemen met een hoog risico zijn bestand tegen pogingen van ongeautoriseerde derden om het gebruik, de outputs of de prestaties ervan te wijzigen door gebruik te maken van de kwetsbaarheden van het systeem.

De technische oplossingen die gericht zijn op het waarborgen van de cyberbeveiliging van AI-systemen met een hoog risico sluiten aan op de relevante omstandigheden en risico's.

De technische oplossingen voor het aanpakken van AI-specifieke kwetsbaarheden omvatten, waar passend, maatregelen voor het voorkomen, traceren, reageren op, oplossen en beheersen van aanvallen waarmee een poging wordt gedaan tot het manipuleren van de dataset voor de training (de zogenaamde “datavervuiling”), van vooraf getrainde componenten die in de training zijn gebruikt (de zogenaamde “modelvervuiling”), van input die is gecreëerd om fouten van het model te veroorzaken (zogenaamde “vijandige voorbeelden” of “modelontwijking”), van aanvallen om vertrouwelijke gegevens te bemachtigen of van tekortkomingen van het model.

AFDELING 3

VERPLICHTINGEN VAN AANBIEDERS EN GEBRUIKSVERANTWOORDELIJKEN VAN AI-SYSTEMEN MET EEN HOOG RISICO EN ANDERE PARTIJEN

Artikel 16

Verplichtingen van aanbieders van AI-systemen met een hoog risico

Aanbieders van AI-systemen met een hoog risico:

- a) zorgen ervoor dat hun AI-systemen met een hoog risico in overeenstemming zijn met de eisen van afdeling 2;
- b) vermelden op het AI-systeem met een hoog risico of, wanneer dit niet mogelijk is, op de verpakking of in de bij het product gevoegde documentatie, naargelang het geval, hun naam, geregistreerde handelsnaam of geregistreerd merk en hun contactadres;
- c) beschikken over een systeem voor kwaliteitsbeheer dat in overeenstemming is met artikel 17;
- d) bewaren de in artikel 18 bedoelde documentatie;
- e) bewaren de in artikel 19 bedoelde logs die automatisch door hun AI-systemen met een hoog risico zijn gegenereerd, wanneer zij hierover de controle hebben;
- f) zorgen ervoor dat voor het AI-systeem met een hoog risico de desbetreffende in artikel 43 bedoelde conformiteitsbeoordelingsprocedure wordt uitgevoerd voordat dit systeem in de handel wordt gebracht of in gebruik wordt gesteld;

- g) stellen een EU-conformiteitsverklaring op, in overeenstemming met artikel 47;
- h) brengen de CE-markering aan op het AI-systeem met een hoog risico of, wanneer dit niet mogelijk is, op de verpakking of in de bij het product gevoegde documentatie, om aan te geven dat aan deze verordening is voldaan, overeenkomstig artikel 48;
- i) leven de registratieverplichtingen als bedoeld in artikel 49, lid 1, na;
- j) nemen de noodzakelijke corrigerende maatregelen en verstrekken de uit hoofde van artikel 20 vereiste informatie;
- k) tonen op een met redenen omkleed verzoek van een nationale bevoegde autoriteit de overeenstemming aan van het AI-systeem met een hoog risico met de eisen van afdeling 2;
- l) zorgen ervoor dat het AI-systeem met een hoog risico voldoet aan de toegankelijkheidseisen overeenkomstig de Richtlijnen (EU) 2016/2102 en (EU) 2019/882.

Artikel 17

Systeem voor kwaliteitsbeheer

1. Aanbieders van AI-systemen met een hoog risico voorzien in een systeem voor kwaliteitsbeheer dat de naleving van deze verordening waarborgt. Dit systeem wordt op systematische en ordelijke wijze gedocumenteerd in de vorm van schriftelijke beleidslijnen, procedures en instructies en omvat ten minste de volgende aspecten:
 - a) een strategie voor de naleving van de regelgeving, inclusief de naleving van de conformiteitsbeoordelingsprocedures en de procedures voor het beheer van de wijzigingen van het AI-systeem met een hoog risico;

- b) technieken, procedures en systematische maatregelen die moeten worden toegepast voor het ontwerp, de controle van het ontwerp en de verificatie van het ontwerp van het AI-systeem met een hoog risico;
- c) technieken, procedures en systematische maatregelen die moeten worden toegepast voor de ontwikkeling, de kwaliteitscontrole en de kwaliteitsborging van het AI-systeem met een hoog risico;
- d) procedures voor het inspecteren, testen en valideren die vóór, tijdens en na de ontwikkeling van het AI-systeem met een hoog risico moeten worden uitgevoerd en de regelmaat waarmee zij moeten worden uitgevoerd;
- e) technische specificaties, met inbegrip van normen, die moeten worden toegepast en, wanneer de relevante geharmoniseerde normen niet volledig worden toegepast of geen betrekking hebben op alle relevante eisen van afdeling 2, de middelen die worden gebruikt om ervoor te zorgen dat het AI-systeem met een hoog risico in overeenstemming is met deze eisen;
- f) systemen en procedures voor databeheer, met inbegrip van dataverwerving, -verzameling, -analyse, -labeling, -opslag, -zuivering, -aggregatie en -behoud en datamining en eventuele andere operaties met betrekking tot de data die worden uitgevoerd voorafgaand aan en met het oog op het in de handel brengen of in gebruik stellen van AI-systemen met een hoog risico;
- g) het systeem voor risicobeheer zoals bedoeld in artikel 9;
- h) het opzetten, toepassen en onderhouden van een systeem voor monitoring na het in de handel brengen, overeenkomstig artikel 72;

- i) procedures in verband met het melden van een ernstig incident in overeenstemming met artikel 73;
 - j) de communicatie met nationale bevoegde autoriteiten, andere relevante autoriteiten, met inbegrip van autoriteiten die de toegang tot data verlenen of ondersteunen, aangemelde instanties, andere operatoren, klanten of andere belanghebbenden;
 - k) systemen en procedures voor de registratie van alle relevante documentatie en informatie;
 - l) het beheer van hulpmiddelen, met inbegrip van maatregelen in verband met de voorzieningszekerheid;
 - m) een kader voor de verantwoording, waarin de verantwoordelijkheden van het management en ander personeel uiteen worden gezet met betrekking tot alle aspecten van dit lid.
2. De uitvoering van de in lid 1 bedoelde aspecten is evenredig aan de omvang van de organisatie van de aanbieder. Aanbieders voldoen hoe dan ook aan de striktheid en het beschermingsniveau die nodig zijn om te garanderen dat hun AI-systemen met een hoog risico aan deze verordening voldoen.
3. Aanbieders van AI-systemen met een hoog risico die onderworpen zijn aan verplichtingen met betrekking tot kwaliteitsbeheersystemen of een gelijkwaardige functie uit hoofde van het desbetreffende sectorale Unierecht, kunnen de in lid 1 genoemde aspecten opnemen als onderdeel van de op grond van dat recht vastgestelde kwaliteitsbeheersystemen.

4. Voor aanbieders die in de hoedanigheid van financiële instellingen onderworpen zijn aan eisen met betrekking tot hun interne governance, regelingen of processen uit hoofde van het desbetreffende Unierecht inzake financiële diensten, wordt met uitzondering van lid 1, punten g), h) en i), van dit artikel de verplichting een systeem voor kwaliteitsbeheer in te voeren geacht te zijn vervuld door te voldoen aan de regels inzake interne governance, regelingen of processen uit hoofde van het desbetreffende Unierecht inzake financiële diensten. Daartoe wordt rekening gehouden met eventuele geharmoniseerde normen als bedoeld in artikel 40.

Artikel 18

Bewaring van documentatie

1. De aanbieder houdt gedurende een periode van tien jaar nadat het AI-systeem met een hoog risico in de handel is gebracht of in gebruik is gesteld de volgende elementen ter beschikking van de nationale bevoegde autoriteiten:
- a) de technische documentatie als bedoeld in artikel 11;
 - b) de documentatie betreffende het in artikel 17 bedoelde systeem voor kwaliteitsbeheer;
 - c) in voorkomend geval de documentatie betreffende de door aangemelde instanties goedgekeurde wijzigingen;
 - d) in voorkomend geval de besluiten en andere documenten die door de aangemelde instanties zijn afgegeven;
 - e) de EU-conformiteitsverklaring als bedoeld in artikel 47.

2. Elke lidstaat stelt de voorwaarden vast waaronder de in lid 1 bedoelde documentatie gedurende de in dat lid genoemde periode ter beschikking van de nationale bevoegde autoriteiten blijft voor de gevallen waarin een aanbieder of zijn op zijn grondgebied gevestigde gemachtigde failliet gaat of zijn activiteiten vóór het verstrijken van die termijn staakt.
3. Aanbieders die in de hoedanigheid van financiële instellingen onderworpen zijn aan eisen met betrekking tot hun interne governance, regelingen of processen uit hoofde van het Unierecht voor financiële diensten, bewaren de technische documentatie als onderdeel van de documentatie die bewaard wordt krachtens het desbetreffende Unierecht inzake financiële diensten.

Artikel 19

Automatisch gegenereerde logs

1. Aanbieders van AI-systemen met een hoog risico bewaren de in artikel 12, lid 1, bedoelde logs die automatisch worden gegenereerd door hun AI-systemen met een hoog risico voor zover dergelijke logs onder hun controle vallen. Onverminderd het toepasselijke Unie- of nationale recht worden deze logs bewaard gedurende een periode, die passend is voor het beoogde doel van het AI-systeem met een hoog risico, van ten minste zes maanden, tenzij anders is bepaald in het toepasselijke Unie- of nationaal recht, met name het Unierecht inzake de bescherming van persoonsgegevens.
2. Aanbieders die in de hoedanigheid van financiële instellingen onderworpen zijn aan eisen met betrekking tot hun interne governance, regelingen of processen uit hoofde van het Unierecht inzake financiële diensten, bewaren de automatisch door hun AI-systemen met een hoog risico gegenereerde logs, als onderdeel van de documentatie die bewaard wordt krachtens het desbetreffende recht inzake financiële diensten.

Artikel 20

Corrigerende maatregelen en mededelingsverplichting

1. Aanbieders van AI-systemen met een hoog risico die van mening zijn of redenen hebben om aan te nemen dat een door hen in de handel gebracht of in gebruik gesteld AI-systeem met een hoog risico niet in overeenstemming is met deze verordening, nemen onmiddellijk de nodige corrigerende maatregelen om dat systeem naargelang het geval in overeenstemming te brengen, uit de handel te nemen, te deactiveren of terug te roepen. Zij stellen de distributeurs van het betrokken AI-systeem met een hoog risico en, indien van toepassing, de gebruiksverantwoordelijken, de gemachtigden en importeurs dienovereenkomstig in kennis.
2. Wanneer het AI-systeem met een hoog risico een risico vormt in de zin van artikel 79, lid 1, en de aanbieder kennis neemt van dat risico, onderzoekt hij onmiddellijk de oorzaken in samenwerking met, in voorkomend geval, de gebruiksverantwoordelijke die het risico heeft gemeld, informeert hij de markttoezichtautoriteiten die bevoegd zijn voor het betrokken AI-systeem met een hoog risico en, in voorkomend geval, de aangemelde instantie die een certificaat voor het AI-systeem met een hoog risico heeft afgegeven overeenkomstig artikel 44, met name over de aard van de non-conformiteit en over eventuele relevante getroffen corrigerende maatregelen.

Artikel 21

Samenwerking met bevoegde autoriteiten

1. Op een met redenen omkleed verzoek van een bevoegde autoriteit, verstrekken aanbieders van AI-systemen met een hoog risico die autoriteit alle informatie en documentatie die noodzakelijk is om de overeenstemming van het AI-systeem met een hoog risico met de eisen van afdeling 2 aan te tonen, in een eenvoudig door de instantie te begrijpen en door de betrokken lidstaat gekozen officiële taal van de instellingen van de Unie.
2. Op een met redenen omkleed verzoek van een bevoegde autoriteit verlenen aanbieders die verzoekende bevoegde autoriteit, indien van toepassing, toegang tot de in artikel 12, lid 1, bedoelde logs die automatisch zijn gegenereerd door hun AI-systeem met een hoog risico voor zover dergelijke logs onder hun controle vallen.
3. De door de bevoegde autoriteit krachtens dit artikel verkregen informatie en documentatie worden verwerkt overeenkomstig de in artikel 78 vastgestelde vertrouwelijkheidsverplichtingen.

Artikel 22

Gemachtigden van aanbieders van AI-systemen met een hoog risico

1. Aanbieders die in derde landen zijn gevestigd, wijzen voordat zij hun AI-systemen met een hoog risico in de Unie in de handel brengen, middels een schriftelijke machtiging een gemachtigde aan die is gevestigd in de Unie.

2. De aanbieder stelt zijn gemachtigde in staat de taken uit te voeren die staan gespecificeerd in het mandaat dat hij van de aanbieder heeft ontvangen.
3. De gemachtigde voert de taken uit die gespecificeerd zijn in het mandaat dat hij van de aanbieder heeft ontvangen. Hij legt op verzoek een kopie van het mandaat over aan de markttoezichtautoriteiten, in een door de bevoegde autoriteit aangegeven officiële taal van de instellingen van de Unie. Voor de toepassing van deze verordening geeft het mandaat de gemachtigde de bevoegdheid om de volgende taken te verrichten:
 - a) nagaan of de in artikel 47 bedoelde EU-conformiteitsverklaring en de in artikel 11 bedoelde technische documentatie zijn opgesteld en of de aanbieder een passende conformiteits-beoordelingsprocedure heeft uitgevoerd;
 - b) gedurende een periode van tien jaar nadat het AI-systeem met een hoog risico in de handel is gebracht of in gebruik is gesteld, de contactgegevens van de aanbieder die de gemachtigde heeft aangewezen alsmede een kopie van de in artikel 47 bedoelde EU-conformiteits-verklaring, de technische documentatie en, in voorkomend geval, het door de aangemelde instantie afgegeven certificaat, ter beschikking houden van de bevoegde autoriteiten en de in artikel 74, lid 10, bedoelde nationale autoriteiten of organen;
 - c) een bevoegde autoriteit op met redenen omkleed verzoek alle informatie en documentatie verstrekken, met inbegrip van de in punt b) van deze alinea bedoelde documentatie, die noodzakelijk is om de overeenstemming van een AI-systeem met een hoog risico met de eisen van afdeling 2 aan te tonen, met inbegrip van de in artikel 12, lid 1, bedoelde logs die automatisch zijn gegenereerd door het AI-systeem met een hoog risico voor zover dergelijke logs onder de controle van de aanbieder vallen;

- d) op met redenen omkleed verzoek samenwerken met bevoegde autoriteiten met betrekking tot alle maatregelen die door deze autoriteiten worden getroffen in verband met het AI-systeem met een hoog risico, met name om de risico's van dat systeem te verminderen en te beperken;
- e) waar toepasselijk, voldoen aan de in artikel 49, lid 1, bedoelde registratieverplichtingen of, indien de registratie door de aanbieder zelf wordt uitgevoerd, waarborgen dat de in bijlage VIII, afdeling A, punt 3, bedoelde informatie juist is.

Door het mandaat wordt de gemachtigde aangesteld als aanspreekpunt, naast of in plaats van de aanbieder, voor de bevoegde autoriteiten, met betrekking tot alle vraagstukken die verband houden met het waarborgen van de naleving van deze verordening.

- 4. De gemachtigde beëindigt het mandaat indien hij van mening is of redenen heeft om aan te nemen dat de aanbieder in strijd met zijn verplichtingen op grond van deze verordening handelt. Hij stelt daar dan, met opgave van redenen, de relevante markttoezichtautoriteit onmiddellijk van in kennis, alsmede, in voorkomend geval, de relevante aangemelde instantie.

Artikel 23

Verplichtingen van importeurs

- 1. Alvorens een AI-systeem met een hoog risico in de handel wordt gebracht, zorgen de importeurs ervoor dat het systeem in overeenstemming is met deze verordening door na te gaan of:
 - a) de relevante conformiteitsbeoordelingsprocedure als bedoeld in artikel 43 is uitgevoerd door de aanbieder van het AI-systeem met een hoog risico;

- b) de aanbieder de technische documentatie heeft opgesteld in overeenstemming met artikel 11 en bijlage IV;
 - c) de vereiste CE-markering op het systeem is aangebracht en het systeem vergezeld gaat van de in artikel 47 bedoelde EU-conformiteitsverklaring en gebruiksaanwijzingen;
 - d) de aanbieder een gemachtigde heeft aangewezen, in overeenstemming met artikel 22, lid 1.
2. Ingeval een importeur afdoende redenen heeft om aan te nemen dat een AI-systeem met een hoog risico niet in overeenstemming is met deze verordening, vervalst is of vergezeld gaat van vervalste documenten, brengt hij het systeem niet in de handel voordat het in overeenstemming is gebracht. Wanneer het AI-systeem met een hoog risico een risico vormt in de zin van artikel 79, lid 1, stelt de importeur de aanbieder van het systeem, de gemachtigden, en de markttoezichtautoriteiten hiervan in kennis.
3. Importeurs vermelden hun naam, geregistreerde handelsnaam of geregistreerd merk en hun contactadres voor het AI-systeem met een hoog risico op de verpakking of in de bij het product gevoegde documentatie, indien van toepassing.
4. Importeurs zorgen gedurende de periode dat zij voor een AI-systeem met een hoog risico verantwoordelijk zijn voor opslag- en vervoersomstandigheden, indien van toepassing, die de overeenstemming van het systeem met de eisen van afdeling 2 niet in het gedrang brengen.

5. Importeurs bewaren gedurende een periode van tien jaar nadat het AI-systeem met een hoog risico in de handel is gebracht of in gebruik is gesteld, een kopie van het door de aangemelde instantie afgegeven certificaat, en in voorkomend geval tevens een kopie van de gebruiksaanwijzing en van de in artikel 47 bedoelde EU-conformiteitsverklaring.
6. Importeurs verstrekken ter staving van de conformiteit van een AI-systeem met een hoog risico met de eisen van afdeling 2, de relevante bevoegde autoriteiten op met redenen omkleed verzoek alle nodige informatie en documentatie, met inbegrip van de in lid 5 bedoelde informatie en documentatie, in een gemakkelijk voor die autoriteit te begrijpen taal. Hiertoe zorgen zij er tevens voor dat aan deze autoriteiten de technische documentatie ter beschikking kan worden gesteld.
7. Importeurs werken met de relevante bevoegde autoriteiten samen met betrekking tot alle maatregelen die door deze autoriteiten worden getroffen in verband met het AI-systeem met een hoog risico dat door de importeurs in de handel is gebracht, met name om de risico's van dat systeem te verminderen en te beperken.

Artikel 24

Verplichtingen van distributeurs

1. Voordat zij een AI-systeem met een hoog risico op de markt aanbieden, controleren distributeurs of daarop de vereiste CE-markering is aangebracht, of het systeem vergezeld gaat van de in artikel 47 bedoelde EU-conformiteitsverklaring en gebruiksinstructies en of de aanbieder en importeur van dat systeem, naargelang het geval, hun respectievelijke verplichtingen als vastgelegd in artikel 16, punten b) en c), en artikel 23, lid 3, hebben nageleefd.

2. Wanneer een distributeur van mening is of redenen heeft om, op grond van de informatie waarover hij beschikt, aan te nemen dat een AI-systeem met een hoog risico niet in overeenstemming is met de eisen van afdeling 2, brengt hij het AI-systeem met een hoog risico niet in de handel voordat het in overeenstemming is gebracht met deze eisen. Daarnaast stelt de distributeur, wanneer het AI-systeem met een hoog risico een risico vormt in de zin van artikel 79, lid 1, de aanbieder of de importeur van het AI-systeem, naargelang als van toepassing, hiervan in kennis.
3. Distributeurs zorgen gedurende de periode waarin zij voor een AI-systeem met een hoog risico verantwoordelijk zijn voor opslag- en vervoersomstandigheden, indien van toepassing, die de overeenstemming van het systeem met de eisen van afdeling 2 niet in het gedrang brengen.
4. Een distributeur die van mening is of redenen heeft om, op grond van de informatie waarover hij beschikt, aan te nemen dat een AI-systeem met een hoog risico dat hij op de markt heeft aangeboden, niet in overeenstemming is met de eisen van afdeling 2, neemt de noodzakelijke corrigerende maatregelen om dat systeem in overeenstemming te brengen met deze eisen, uit de handel te nemen of terug te roepen of zorgt ervoor dat de aanbieder, de importeur of een eventuele betrokken operator, waar passend, dergelijke corrigerende maatregelen treft. Indien het AI-systeem met een hoog risico een risico vormt in de zin van artikel 79, lid 1, stelt de distributeur de aanbieder of importeur van het systeem en de autoriteiten die bevoegd zijn voor het betreffende AI-systeem met een hoog risico hiervan onmiddellijk in kennis, waarbij hij in het bijzonder de non-conformiteit en de eventueel getroffen corrigerende maatregelen uitvoerig beschrijft.

5. Op een met redenen omkleed verzoek van een relevante bevoegde autoriteit verstrekken distributeurs van een AI-systeem met een hoog risico die autoriteit alle informatie en documentatie met betrekking tot de op grond van de leden 1 tot en met 4 door hen genomen maatregelen die nodig zijn om aan te tonen dat het systeem voldoet aan de eisen van afdeling 2.
6. Distributeurs werken met de relevante bevoegde autoriteiten samen met betrekking tot alle maatregelen die door deze autoriteiten worden getroffen in verband met het AI-systeem met een hoog risico dat door de distributeurs op de markt is aangeboden, met name om de risico's van dat systeem te verminderen of te beperken.

Artikel 25

Verantwoordelijkheden in de AI-waardeketen

1. In de volgende omstandigheden wordt een distributeur, importeur, gebruiksverantwoordelijke of derde voor de toepassing van deze verordening beschouwd als een aanbieder van een AI-systeem met een hoog risico en is hij onderworpen aan de verplichtingen van de aanbieder uit hoofde van artikel 16:
 - a) hij zet zijn naam of merk op een AI-systeem met een hoog risico dat reeds in de handel is gebracht of in gebruik is gesteld, onverminderd contractuele regelingen waarin wordt bepaald dat de verplichtingen anders worden toegewezen;
 - b) hij brengt een substantiële wijziging aan in een AI-systeem met een hoog risico dat reeds in de handel is gebracht of reeds in gebruik is gesteld op zodanige wijze dat het systeem een AI-systeem met een hoog risico blijft op grond van artikel 6;

c) hij wijzigt het beoogde doel van een AI-systeem, met inbegrip van een AI-systeem voor algemene doeleinden, dat niet als een systeem met een hoog risico is geclassificeerd en reeds in de handel is gebracht of in gebruik is gesteld, op zodanige wijze dat het betrokken AI-systeem een AI-systeem met een hoog risico overeenkomstig artikel 6 wordt.

2. Wanneer sprake is van de in lid 1 bedoelde omstandigheden, wordt de aanbieder die het AI-systeem voor het eerst in de handel heeft gebracht of in gebruik heeft gesteld, niet langer beschouwd als aanbieder van dat specifieke AI-systeem voor de toepassing van deze verordening. Die oorspronkelijke aanbieder werkt nauw samen met nieuwe aanbieders, stelt de nodige informatie beschikbaar en verstrekt de redelijkerwijs verwachte technische toegang en andere bijstand die nodig zijn om te voldoen aan de verplichtingen van deze verordening, met name wat betreft de naleving van de conformiteitsbeoordeling van AI-systemen met een hoog risico. Dit lid is niet van toepassing in gevallen waarin de oorspronkelijke aanbieder duidelijk heeft aangegeven dat zijn AI-systeem niet mag worden gewijzigd in een AI-systeem met een hoog risico en derhalve niet onder de verplichting valt om de documentatie te verstrekken.

3. Bij AI-systemen met een hoog risico die veiligheidscomponenten van producten zijn die vallen onder de in bijlage I, afdeling A, genoemde harmonisatiewetgeving van de Unie, wordt de productfabrikant beschouwd als de aanbieder van het AI-systeem met een hoog risico en is hij onderworpen aan de verplichtingen krachtens artikel 16 in een van de volgende situaties:

- a) het AI-systeem met een hoog risico wordt samen met het product onder de naam of het merk van de productfabrikant in de handel gebracht;
- b) het AI-systeem met een hoog risico wordt onder de naam of het merk van de productfabrikant in gebruik gesteld nadat het product in de handel is gebracht.

4. De aanbieder van een AI-systeem met een hoog risico en de derde partij die instrumenten, diensten, onderdelen of processen voor AI-systemen levert die worden gebruikt of geïntegreerd in een AI-systeem met een hoog risico, preciseren in een schriftelijke overeenkomst de nodige informatie, capaciteiten, technische toegang en andere bijstand, op basis van de algemeen erkende stand van de techniek, om de aanbieder van het AI-systeem met een hoog risico in staat te stellen volledig te voldoen aan de verplichtingen van deze verordening. Dit lid is niet van toepassing op derden die andere instrumenten, diensten, processen of onderdelen dan AI-modellen voor algemene doeleinden onder een vrije en opensource licentie toegankelijk maken voor het publiek.

Het AI-bureau kan vrijwillige modelvoorwaarden ontwikkelen en aanbevelen voor contracten tussen aanbieders van AI-systemen met een hoog risico en derden die instrumenten, diensten, componenten of processen leveren die worden gebruikt of geïntegreerd in AI-systemen met een hoog risico. Bij de ontwikkeling van die vrijwillige modelvoorwaarden moet het AI-bureau rekening houden met de contractuele eisen die kunnen gelden in specifieke sectoren of businesscases. De vrijwillige modelvoorwaarden worden gepubliceerd en kosteloos beschikbaar gesteld in een gemakkelijk bruikbaar elektronisch formaat.

5. De leden 2 en 3 doen geen afbreuk aan de noodzaak om intellectuele-eigendomsrechten, vertrouwelijke bedrijfsinformatie en bedrijfsgeheimen te eerbiedigen en te beschermen overeenkomstig het Unierecht en het nationale recht.

Artikel 26

Verplichtingen van gebruiksverantwoordelijken van AI-systemen met een hoog risico

1. Gebruiksverantwoordelijken van AI-systemen met een hoog risico nemen passende technische en organisatorische maatregelen om te waarborgen dat zij dergelijke systemen gebruiken in overeenstemming met de gebruiksaanwijzingen die bij de systemen zijn gevoegd, op grond van de leden 3 en 6.

2. Gebruiksverantwoordelijken dragen het menselijk toezicht op aan natuurlijke personen die over de nodige bekwaamheid, opleiding en autoriteit beschikken en de nodige ondersteuning krijgen.
3. De verplichtingen van de leden 1 en 2 doen geen afbreuk aan andere verplichtingen van gebruiksverantwoordelijken op grond van het Unie- of nationaal recht en aan de vrijheid van gebruiksverantwoordelijken om hun eigen middelen en activiteiten te organiseren voor de uitvoering van de maatregelen inzake menselijk toezicht zoals aangegeven door de aanbieder.
4. Onverminderd de leden 1 en 2 zorgt de gebruiksverantwoordelijke, voor zover hij controle heeft over de inputdata, ervoor dat de inputdata relevant en voldoende representatief zijn voor het beoogde doel van het AI-systeem met een hoog risico.
5. Gebruiksverantwoordelijken monitoren de werking van het AI-systeem met een hoog risico op basis van de gebruiksaanwijzingen en stellen in voorkomend geval de aanbieders in kennis overeenkomstig artikel 72. Wanneer gebruiksverantwoordelijken redenen hebben om aan te nemen dat het gebruik overeenkomstig de gebruiksaanwijzingen ertoe kan leiden dat dat AI-systeem een risico vormt in de zin van artikel 79, lid 1, stellen zij de aanbieder of distributeur en de betreffende markttoezichtautoriteit hiervan zonder onnodige vertraging in kennis en onderbreken zij het gebruik van dat systeem. Wanneer gebruiksverantwoordelijke een ernstig incident vaststellen, stellen zij ook onmiddellijk eerst de aanbieder hiervan in kennis, en vervolgens de importeur of distributeur en de betreffende markttoezichtautoriteiten van dat incident. Wanneer de gebruiksverantwoordelijke de aanbieder niet kan bereiken, is artikel 73 mutatis mutandis van toepassing. Deze verplichting geldt niet voor gevoelige operationele gegevens van gebruiksverantwoordelijke van AI-systemen die de hoedanigheid van rechtshandhavingsinstanties hebben.

Voor gebruiksverantwoordelijke die in de hoedanigheid van financiële instellingen onderworpen zijn aan eisen met betrekking tot hun interne governance, regelingen of processen uit hoofde van het Unierecht inzake financiële diensten, wordt de monitoringsverplichting overeenkomstig de eerste alinea geacht te zijn vervuld door te voldoen aan de regels inzake interne governance, regelingen of processen en -mechanismen uit hoofde van het desbetreffende recht inzake financiële diensten.

6. Gebruiksverantwoordelijken van AI-systemen met een hoog risico bewaren de logs die automatisch worden gegenereerd door dat AI-systeem met een hoog risico voor zover dergelijke logs onder hun controle vallen gedurende een periode die passend is voor het beoogde doel van het AI-systeem met een hoog risico, of ten minste zes maanden, tenzij anders is bepaald in het toepasselijke Unie- of nationaal recht, meer in het bijzonder het Unierecht over de bescherming van persoonsgegevens.

Gebruiksverantwoordelijken die in de hoedanigheid van financiële instellingen onderworpen zijn aan eisen met betrekking tot hun interne governance, regelingen of processen uit hoofde van het Unierecht inzake financiële diensten bewaren de logs als onderdeel van de documentatie die bewaard wordt krachtens het desbetreffende Unierecht inzake financiële diensten.

7. Voordat een AI-systeem met een hoog risico op de werkplek in gebruik wordt gesteld of wordt gebruikt, delen gebruiksverantwoordelijken die werkgever zijn werknemersvertegenwoordigers en de betrokken werknemers mee dat zij zullen worden onderworpen aan het gebruik van het AI-systeem met een hoog risico. Deze informatie wordt, indien van toepassing, verstrekt in overeenstemming met de in het Unie- en nationaal recht vastgelegde regels en procedures en de praktijk inzake informatie van werknemers en hun vertegenwoordigers.

8. Gebruiksverantwoordelijken van AI-systemen met een hoog risico die de hoedanigheid van overheidsinstanties of instellingen, organen of instanties van de Unie hebben, leven de in artikel 49 bedoelde registratieverplichtingen na. Wanneer deze gebruiksverantwoordelijke vaststellen dat het AI-systeem met een hoog risico dat zij voornemens zijn te gebruiken niet in de in artikel 71 bedoelde EU-databank is geregistreerd, gebruiken zij dat systeem niet en stellen zij de aanbieder of de distributeur daarvan in kennis.
9. Indien van toepassing, gebruiken gebruiksverantwoordelijken van AI-systemen met een hoog risico de informatie die op grond van artikel 13 van deze verordening wordt verstrekt om hun verplichting na te komen om een gegevensbeschermingseffectbeoordeling uit te voeren op grond van artikel 35 van Verordening (EU) 2016/679 of artikel 27 van Richtlijn (EU) 2016/680.
10. Onverminderd Richtlijn (EU) 2016/680 verzoekt de gebruiksverantwoordelijke van een AI-systeem met een hoog risico voor biometrische identificatie op afstand achteraf in het kader van een onderzoek waarbij gericht wordt gezocht naar een persoon die wordt verdacht van of veroordeeld is voor het plegen van een strafbaar feit, vooraf of zonder onnodige vertraging en uiterlijk 48 uur na het feit, om toestemming van een gerechtelijke instantie of administratieve instantie, van wie de beslissing bindend is en onderworpen is aan rechterlijke toetsing, voor het gebruik van dat systeem, behalve wanneer het wordt gebruikt voor de initiële identificatie van een potentiële verdachte op basis van objectieve en verifieerbare feiten die rechtstreeks verband houden met het strafbare feit. Elk gebruik wordt beperkt tot hetgeen strikt noodzakelijk is voor het onderzoek naar een specifiek strafbaar feit.

Indien de op grond van de eerste alinea verzochte toestemming wordt geweigerd, wordt het gebruik van het systeem voor biometrische identificatie op afstand achteraf dat verband houdt met de verzochte toestemming met onmiddellijke ingang stopgezet en worden de persoonsgegevens die verband houden met het gebruik van het AI-systeem met een hoog risico waarvoor de toestemming is gevraagd, gewist.

Een dergelijk AI-systeem met een hoog risico voor biometrische identificatie op afstand achteraf mag in geen geval op niet-gerichte wijze worden gebruikt voor rechtshandavingsdoeleinden, zonder enig verband met een strafbaar feit, een strafrechtelijke procedure, een werkelijke en actuele of werkelijke en te verwachten dreiging van een strafbaar feit, of zoektocht naar een specifieke vermiste persoon. Er moet voor worden gezorgd dat rechtshandavingsinstanties geen enkel besluit met nadelige rechtsgevolgen voor een persoon mogen nemen op basis van uitsluitend de output van dergelijke systemen voor biometrische identificatie op afstand achteraf.

Deze alinea doet geen afbreuk aan artikel 9 van Verordening (EU) 2016/679 en artikel 10 van Richtlijn (EU) 2016/680 voor de verwerking van biometrische gegevens.

Ongeacht het doel of de gebruiksverantwoordelijke wordt elk gebruik van dergelijke AI-systemen met een hoog risico gedocumenteerd in het desbetreffende politiedossier en op verzoek ter beschikking gesteld van de relevante markttoezichtautoriteit en de nationale gegevensbeschermingsautoriteit, met uitzondering van gevoelige operationele gegevens in verband met rechtshandhaving. Deze alinea doet geen afbreuk aan de bij Richtlijn (EU) 2016/680 aan de toezichthoudende autoriteiten verleende bevoegdheden.

Gebruiksverantwoordelijken dienen bij de relevante markttoezichtautoriteiten en de nationale gegevensbeschermingsautoriteiten jaarverslagen in over hun gebruik van systemen voor biometrische identificatie op afstand achteraf, met uitzondering van gevoelige operationele gegevens in verband met rechtshandhaving. De verslagen kunnen worden samengevoegd, zodat ze informatie bevatten over meerdere soorten van inzetten.

De lidstaten kunnen, in overeenstemming met het Unierecht, beperkendere wetgeving invoeren inzake het gebruik van systemen voor biometrische identificatie op afstand achteraf.

11. Onverminderd artikel 50 van deze verordening informeren gebruiksverantwoordelijken van in bijlage III bedoelde AI-systemen met een hoog risico die beslissingen met betrekking tot natuurlijke personen nemen of helpen nemen, de natuurlijke personen dat het AI-systeem met een hoog risico op hen wordt toegepast. Op AI-systemen met een hoog risico die voor rechtshandavingsdoeleinden worden gebruikt, is artikel 13 van Richtlijn (EU) 2016/680 van toepassing.
12. Gebruiksverantwoordelijken werken samen met de relevante bevoegde autoriteiten bij alle door deze autoriteiten genomen maatregelen met betrekking tot een AI-systeem met een hoog risico met het oog op de uitvoering van deze verordening.

Artikel 27

Beoordeling van de gevolgen voor de grondrechten van AI-systemen met een hoog risico

1. Voordat een AI-systeem met een hoog risico als bedoeld in artikel 6, lid 2, in gebruik wordt gesteld, met uitzondering van AI-systemen met een hoog risico die bedoeld zijn om te worden gebruikt op het in punt 2 van bijlage III vermelde gebied, voeren gebruiksverantwoordelijken die publiekrechtelijke organen zijn of particuliere entiteiten zijn die openbare diensten verlenen, en gebruiksverantwoordelijken van AI-systemen met een hoog risico als bedoeld in bijlage III, punt 5, onder b) en c), een beoordeling uit van de gevolgen voor de grondrechten die het gebruik van een dergelijk systeem kan opleveren. Daartoe voeren gebruiksverantwoordelijken een beoordeling uit die bestaat uit:
 - a) een beschrijving van de processen van de gebruiksverantwoordelijke waarbij het AI-systeem met een hoog risico zal worden gebruikt in overeenstemming met het beoogde doel ervan;
 - b) een beschrijving van de periode waarbinnen en de frequentie waarmee elk AI-systeem met een hoog risico zal worden gebruikt;

- c) categorieën van natuurlijke personen en groepen die naar verwachting gevolgen zullen ondervinden van het gebruik van het systeem in een specifieke context;
- d) de specifieke risico's op schade die waarschijnlijk gevolgen zullen hebben voor de op grond van punt c) van dit lid geïdentificeerde categorieën natuurlijke personen of groepen personen, rekening houdend met de door de aanbieder op grond van artikel 13 verstrekte informatie;
- e) een beschrijving van de uitvoering van maatregelen voor menselijk toezicht, overeenkomstig de gebruiksaanwijzing;
- f) de maatregelen die moeten worden genomen wanneer die risico's zich voordoen, met inbegrip van de regelingen voor interne governance en klachtenregelingen.

2. De verplichting als neergelegd in lid 1 is van toepassing op het eerste gebruik van een AI-systeem met een hoog risico. De gebruiksverantwoordelijke kan in soortgelijke gevallen gebruik maken van eerder uitgevoerde effectbeoordelingen op het gebied van de grondrechten of bestaande effectbeoordelingen die door de aanbieder zijn uitgevoerd. Indien de gebruiksverantwoordelijke tijdens het gebruik van het AI-systeem met een hoog risico ziet dat een van de in lid 1 vermelde elementen is gewijzigd of niet langer actueel is, neemt de gebruiksverantwoordelijke de nodige maatregelen om de informatie te actualiseren.
3. Zodra de in lid 1 van dit artikel bedoelde beoordeling is uitgevoerd, stelt de gebruiksverantwoordelijke de markttoezichtautoriteit in kennis van de resultaten ervan, en dient hij als onderdeel van de kennisgeving het in lid 5 van dit artikel bedoelde ingevulde sjabloon in. In het in artikel 46, lid 1, bedoelde geval kunnen gebruiksverantwoordelijken van de verplichting tot kennisgeving worden vrijgesteld.

4. Indien een van de in dit artikel vastgelegde verplichtingen reeds is nagekomen door de gegevensbeschermingseffectbeoordeling die is uitgevoerd op grond van artikel 35 van Verordening (EU) 2016/679 of artikel 27 van Richtlijn (EU) 2016/680, vormt de in lid 1 van dit artikel bedoelde effectbeoordeling op het gebied van de grondrechten een aanvulling op die gegevensbeschermingseffectbeoordeling.
5. Het AI-bureau ontwikkelt een sjabloon voor een vragenlijst, onder meer via een geautomatiseerd instrument, om gebruiksverantwoordelijken te helpen hun verplichtingen uit hoofde van dit artikel op vereenvoudigde wijze na te komen.

AFDELING 4

AANMELDENDE AUTORITEITEN EN AANGEMELDE INSTANTIES

Artikel 28

Aanmeldende autoriteiten

1. Elke lidstaat wijst ten minste één anmeldende autoriteit aan of richt een anmeldende autoriteit op die verantwoordelijk is voor het opzetten en uitvoeren van de nodige procedures voor de beoordeling, aanwijzing en aanmelding van conformiteitsbeoordelingsinstanties en voor het toezicht erop. Deze procedures worden ontwikkeld in samenwerking tussen de anmeldende autoriteiten van alle lidstaten.
2. De lidstaten kunnen besluiten de beoordeling en het toezicht als bedoeld in lid 1 overeenkomstig Verordening (EG) nr. 765/2008 te laten uitvoeren door een nationale accreditatie-instantie in de zin van die verordening.

3. Aanmeldende autoriteiten worden zodanig opgericht en georganiseerd en functioneren zodanig dat zich geen belangenconflicten met conformiteitsbeoordelingsinstanties voordoen en dat de objectiviteit en onpartijdigheid van hun activiteiten gewaarborgd zijn.
4. Aanmeldende autoriteiten worden zodanig georganiseerd dat besluiten in verband met de aanmelding van conformiteitsbeoordelingsinstanties worden genomen door bekwame personen die niet de beoordeling van die instanties hebben verricht.
5. Aanmeldende autoriteiten bieden of verrichten geen activiteiten die worden uitgevoerd door conformiteitsbeoordelingsinstanties en verlenen geen adviezen op commerciële of concurrentiële basis.
6. Aanmeldende autoriteiten waarborgen dat de door hen verkregen informatie overeenkomstig artikel 78 vertrouwelijk wordt behandeld.
7. Aanmeldende autoriteiten beschikken over een toereikend aantal bekwame personeelsleden om hun taken naar behoren uit te voeren. Bekwame personeelsleden beschikken, indien van toepassing, over de nodige deskundigheid voor hun functies op gebieden als informatietechnologie, AI en recht, met inbegrip van het toezicht op de grondrechten.

Artikel 29

Verzoek om aanmelding van een conformiteitsbeoordelingsinstantie

1. Conformiteitsbeoordelingsinstanties dienen een verzoek om aanmelding in bij de aanmeldende autoriteit van de lidstaat waar zij zijn gevestigd.

2. Het verzoek om aanmelding gaat vergezeld van een beschrijving van de conformiteitsbeoordelingsactiviteiten, de conformiteitsbeoordelingsmodule(s) en de soorten AI-systemen waarvoor de conformiteitsbeoordelingsinstantie verklaart bekwaam te zijn en, indien dit bestaat, van een accreditatiecertificaat dat is afgegeven door een nationale accreditatie-instantie, waarin wordt verklaard dat de conformiteitsbeoordelingsinstantie voldoet aan de eisen van artikel 31.

Geldige documenten met betrekking tot bestaande aanwijzingen van de verzoekende aangemelde instantie uit hoofde van andere harmonisatiewetgeving van de Unie worden bijgevoegd.

3. Wanneer de betrokken conformiteitsbeoordelingsinstantie geen accreditatiecertificaat kan overleggen, verschaft zij de aanmeldende autoriteit alle bewijsstukken die nodig zijn om haar overeenstemming met de eisen van artikel 31 te verifiëren en te erkennen en om daar geregeld toezicht op te houden.
4. Voor aangemelde instanties die uit hoofde van andere harmonisatiewetgeving van de Unie zijn aangewezen, kunnen waar passend alle documenten en certificaten met betrekking tot die aanwijzingen worden gebruikt om hun aanwijzingsprocedure krachtens deze verordening te ondersteunen. Om de voor aangemelde instanties verantwoordelijke autoriteit in staat te stellen de continue naleving van alle eisen van artikel 31 te monitoren en te verifiëren, werkt de aangemelde instantie de in de leden 2 en 3 bij dit artikel bedoelde documentatie telkens bij wanneer relevante veranderingen plaatsvinden.

Artikel 30
Aanmeldingsprocedure

1. Aanmeldende autoriteiten mogen uitsluitend conformiteitsbeoordelingsinstanties aanmelden die aan de eisen van artikel 31 voldoen.
2. Aanmeldende autoriteiten melden elke in lid 1 bedoeld conformiteitsbeoordelingsinstantie aan bij de Commissie en de andere lidstaten door middel van het door de Commissie ontwikkelde en beheerde elektronische aanmeldingssysteem.
3. Bij de in lid 2 van dit artikel bedoelde aanmelding worden de conformiteitsbeoordelingsactiviteiten, de conformiteitsbeoordelingsmodule(s), de soorten AI-systemen in kwestie en de desbetreffende bekwaamheidsattestatie uitvoerig beschreven. Indien een aanmelding niet gebaseerd is op een accreditatiecertificaat als bedoeld in artikel 29, lid 2, verschaft de aanmeldende autoriteit de Commissie en de andere lidstaten de bewijsstukken waaruit de bekwaamheid van de conformiteitsbeoordelingsinstantie blijkt, evenals de regeling die waarborgt dat de instantie regelmatig wordt gecontroleerd en zal blijven voldoen aan de eisen van artikel 31.
4. De betrokken conformiteitsbeoordelingsinstantie mag de activiteiten van een aangemelde instantie alleen verrichten als de Commissie en de andere lidstaten binnen twee weken na aanmelding door een aanmeldende autoriteit indien een accreditatiecertificaat bedoeld in artikel 29, lid 2, wordt gebruikt en binnen twee maanden na aanmelding door de aanmeldende autoriteit indien de in artikel 29, lid 3, bedoelde bewijsstukken worden gebruikt, geen bezwaren hebben ingediend.

5. Indien er bezwaar wordt ingediend, treedt de Commissie onverwijld in overleg met de betrokken lidstaten en de conformiteitsbeoordelingsinstantie. Met het oog daarop besluit de Commissie of de toelating gerechtvaardigd is. De Commissie richt haar besluit aan de betrokken lidstaat en aan de relevante conformiteitsbeoordelingsinstantie.

Artikel 31

Voorschriften in verband met aangemelde instanties

1. Een aangemelde instantie wordt naar het recht van een lidstaat opgericht en bezit rechtspersoonlijkheid.
2. Aangemelde instanties voldoen aan de eisen inzake organisatie, kwaliteitsbeheer, personeel en processen die nodig zijn voor het vervullen van hun taken, alsook aan de passende cyberbeveiligingseisen.
3. De organisatiestructuur, de toewijzing van verantwoordelijkheden, de rapportagelijnen en het functioneren van aangemelde instanties moeten ervoor zorgen dat er vertrouwen is in hun uitvoering en de resultaten van de conformiteitsbeoordelingsactiviteiten die de aangemelde instanties verrichten.
4. Aangemelde instanties zijn onafhankelijk van de aanbieder van een AI-systeem met een hoog risico met betrekking waartoe de aanbieder conformiteitsbeoordelingsactiviteiten verricht. Aangemelde instanties zijn ook onafhankelijk van andere operatoren die een economisch belang hebben in beoordeelde AI-systemen met een hoog risico, alsook van concurrenten van de aanbieder. Dit belet echter niet dat beoordeelde AI-systemen met een hoog risico die nodig zijn voor activiteiten van de conformiteitsbeoordelingsinstantie worden gebruikt of dat dergelijke AI-systemen met een hoog risico voor persoonlijke doeleinden worden gebruikt.

5. Een conformiteitsbeoordelingsinstantie, haar hoogste leidinggevend en het personeel dat de conformiteitsbeoordelingstaken verricht, zijn niet rechtstreeks of als vertegenwoordiger van de betrokken partijen betrokken bij het ontwerpen, ontwikkelen, verhandelen of gebruiken van de AI-systemen met een hoog risico. Zij oefent geen activiteiten uit die de onafhankelijkheid van haar oordeel of haar integriteit met betrekking tot de conformiteitsbeoordelingsactiviteiten waarvoor zij is aangemeld in het gedrang kunnen brengen. Dit geldt met name voor adviesdiensten.
6. Aangemelde instanties worden zodanig georganiseerd en functioneren zodanig dat de onafhankelijkheid, objectiviteit en onpartijdigheid van hun activiteiten gewaarborgd zijn. Aangemelde instanties documenteren en implementeren een structuur en procedures voor het waarborgen van de onpartijdigheid en voor het bevorderen en toepassen van de onpartijdigheidsbeginselen in hun gehele organisatie, onder het personeel en in de beoordelingsactiviteiten.
7. Aangemelde instanties beschikken over gedocumenteerde procedures die waarborgen dat hun personeel, comités, dochterondernemingen, onderaannemers, geassocieerde instanties of personeel van externe instanties overeenkomstig artikel 78 de informatie die zij tijdens conformiteitsbeoordelingsactiviteiten in hun bezit krijgen vertrouwelijk houden, behalve wanneer de openbaarmaking ervan wettelijk vereist is. Het personeel van aangemelde instanties is gebonden aan het beroepsgeheim ten aanzien van alle informatie waarvan het kennis neemt bij de uitoefening van de taken uit hoofde van deze verordening, behalve ten opzichte van de anmeldende autoriteiten van de lidstaat waar de activiteiten plaatsvinden.

8. Aangemelde instanties beschikken over de nodige procedures voor de uitoefening van hun activiteiten, waarin voldoende rekening wordt gehouden met de omvang van een aanbieder, de sector waarin deze actief is, de structuur en de relatieve complexiteit van het betreffende AI-systeem.
9. Aangemelde instanties sluiten voor hun conformiteitsbeoordelingsactiviteiten een passende aansprakelijkheidsverzekering af, tenzij de wettelijke aansprakelijkheid krachtens het nationale recht door de lidstaat van vestiging wordt gedekt of die lidstaat zelf rechtstreeks verantwoordelijk is voor de conformiteitsbeoordeling.
10. Aangemelde instanties zijn in staat al hun taken uit hoofde van deze verordening te verrichten met de grootste mate van beroepsintegriteit en met de vereiste bekwaamheid op het specifieke gebied, ongeacht of deze taken door de aangemelde instanties zelf dan wel namens hen en onder hun verantwoordelijkheid worden verricht.
11. Aangemelde instanties beschikken over voldoende interne deskundigheid om de namens hen door externe partijen verrichte taken doeltreffend te kunnen evalueren. De aangemelde instantie moet permanent beschikken over voldoende administratief, technisch, juridisch en wetenschappelijk personeel dat ervaring heeft met en kennis over de relevante soorten AI-systemen, gegevens en gegevensverwerking en de voorschriften van afdeling 2.
12. Aangemelde instanties nemen deel aan coördinatieactiviteiten als bedoeld in artikel 38. Zij nemen ook rechtstreeks deel aan of worden vertegenwoordigd in Europese normalisatie-instellingen of zorgen ervoor op de hoogte te zijn van actuele relevante normen.

Artikel 32

Vermoeden van conformiteit met voorschriften met betrekking tot aangemelde instanties

Wanneer een conformiteitsbeoordelingsinstantie aantoonst dat zij voldoet aan de criteria in de ter zake doende geharmoniseerde normen of delen ervan, waarvan de referentienummers in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, wordt zij geacht aan de eisen van artikel 31 te voldoen, op voorwaarde dat de van toepassing zijnde geharmoniseerde normen deze eisen dekken.

Artikel 33

Dochterondernemingen van aangemelde instanties en onderaanneming

1. Wanneer de aangemelde instantie specifieke taken in verband met de conformiteitsbeoordeling door een onderaannemer of door een dochteronderneming laat uitvoeren, waarborgt zij dat de onderaannemer of dochteronderneming aan de eisen van artikel 31 voldoet, en brengt zij de anmeldende autoriteit hiervan op de hoogte.
2. Aangemelde instanties nemen de volledige verantwoordelijkheid op zich voor de door onderaannemers of dochterondernemingen verrichte taken.
3. Activiteiten mogen uitsluitend met instemming van de aanbieder door een onderaannemer of dochteronderneming worden uitgevoerd. Aangemelde instanties maken een lijst van hun dochterondernemingen openbaar.
4. De relevante documenten betreffende de beoordeling van de kwalificaties van de onderaannemer of dochteronderneming en de door hen uit hoofde van deze verordening uitgevoerde werkzaamheden worden gedurende een periode van vijf jaar vanaf de einddatum van de onderaanneming ter beschikking van de anmeldende autoriteit gehouden.

Artikel 34

Operationele verplichtingen van aangemelde instanties

1. Aangemelde instanties controleren de conformiteit van AI-systemen met een hoog risico overeenkomstig de conformiteitsbeoordelingsprocedures van artikel 43.
2. Aangemelde instanties vermijden onnodige lasten voor aanbieders bij de uitvoering van hun activiteiten en houden terdege rekening met de omvang van de aanbieder, de sector waarin hij actief is, zijn structuur en de mate van complexiteit van het betrokken AI-systeem met een hoog risico, met name om de administratieve lasten en nalevingskosten voor micro- en kleine ondernemingen in de zin van Aanbeveling 2003/361/EG tot een minimum te beperken. De aangemelde instantie eerbiedigt echter de striktheid en het beschermingsniveau die nodig zijn opdat het AI-systeem met een hoog risico voldoet aan de eisen van deze verordening.
3. Aangemelde instanties stellen alle relevante documentatie, waaronder de documentatie van de aanbieder, ter beschikking van de in artikel 28 bedoelde aanmeldende autoriteit, en verstrekken die aan haar op verzoek, teneinde haar in staat te stellen haar beoordelings-, aanwijzings-, kennisgevings- en monitoringsactiviteiten te verrichten, en de in deze afdeling beschreven beoordeling te vergemakkelijken.

Artikel 35

Identificatienummers en lijsten van aangemelde instanties

1. De Commissie kent elke aangemelde instantie één enkel identificatienummer toe, zelfs wanneer een instantie op grond van meer dan één handeling van de Unie is aangemeld.

2. De Commissie maakt de lijst van krachtens deze verordening aangemelde instanties openbaar, onder vermelding van hun identificatienummers en de activiteiten waarvoor zij zijn aangemeld. De Commissie zorgt ervoor dat de lijst actueel blijft.

Artikel 36

Wijzigingen in de aanmelding

1. De aanmeldende autoriteit stelt de Commissie en de andere lidstaten via het in artikel 30, lid 2, bedoelde elektronische aanmeldingssysteem in kennis van alle relevante wijzigingen in de aanmelding van een aangemelde instantie.
2. De in artikel 29 en artikel 30 vastgelegde procedures zijn van toepassing op uitbreidingen van de reikwijdte van de aanmelding.

Voor andere wijzigingen met betrekking tot de aanmelding dan uitbreidingen van de reikwijdte, zijn de procedures van de leden 3 tot en met 9 van toepassing.

3. Indien een aangemelde instantie besluit haar conformiteitsbeoordelingsactiviteiten stop te zetten, brengt zij de aanmeldende autoriteit en de betrokken aanbieders zo snel mogelijk, en in het geval van een geplande stopzetting minstens één jaar voor de stopzetting van haar activiteiten, daarvan op de hoogte. De certificaten van de aangemelde instantie kunnen gedurende een periode van negen maanden na de stopzetting van de activiteiten van de aangemelde instantie geldig blijven, op voorwaarde dat een andere aangemelde instantie schriftelijk heeft bevestigd dat zij de verantwoordelijkheid voor de AI-systemen met een hoog risico waarop die certificaten betrekking hebben, op zich zal nemen. Die laatste aangemelde instantie verricht vóór het einde van die periode van negen maanden een volledige beoordeling van de betrokken AI-systemen met een hoog risico, alvorens er nieuwe certificaten voor af te leveren. Ingeval de aangemelde instantie haar activiteiten heeft gestaakt, trekt de aanmeldende autoriteit de aanwijzing in.

4. Wanneer een aanmeldende autoriteit voldoende reden heeft om van mening te zijn dat een aangemelde instantie niet meer aan de eisen van artikel 31 voldoet of haar verplichtingen niet nakomt, moet de aanmeldende autoriteit de kwestie onverwijld zo zorgvuldig mogelijk onderzoeken. In die context stelt zij de betrokken aangemelde instantie in kennis van de geopperde bezwaren en biedt zij haar de mogelijkheid haar standpunten kenbaar te maken. Als de aanmeldende autoriteit tot de conclusie komt dat de aangemelde instantie niet meer aan de eisen van artikel 31 voldoet of haar verplichtingen niet nakomt, wordt de aanwijzing door haar beperkt, geschorst of ingetrokken, als passend, afhankelijk van de ernst van het niet naleven van die eisen of verplichtingen. Zij brengt de Commissie en de andere lidstaten daar onmiddellijk van op de hoogte.
5. Indien de aanwijzing van een aangemelde instantie wordt geschorst, beperkt of geheel of gedeeltelijk wordt ingetrokken, stelt die aangemelde instantie de betrokken aanbieders binnen tien dagen hiervan in kennis.
6. Indien een aanwijzing wordt beperkt, geschorst of ingetrokken, onderneemt de aanmeldende autoriteit de nodige stappen om ervoor te zorgen dat de dossiers van de betrokken aangemelde instantie worden bewaard en op verzoek ter beschikking worden gesteld van aanmeldende autoriteiten in andere lidstaten en van markttoezichtautoriteiten.
7. In geval van beperking, schorsing of intrekking van een aanwijzing:
 - a) beoordeelt de aanmeldende autoriteit het gevolg voor de door de aangemelde instantie afgegeven certificaten;
 - b) dient de aanmeldende autoriteit binnen drie maanden na mededeling van de wijzigingen in de aanwijzing een verslag over haar bevindingen in bij de Commissie en de overige lidstaten;

- c) schrijft de aanmeldende autoriteit voor dat de aangemelde instantie binnen een redelijke, door de autoriteit bepaalde termijn, onterecht afgegeven certificaten schorst of intrekt, zulks om de voortdurende conformiteit van de in de handel gebrachte AI-systemen met een hoog risico te waarborgen;
- d) stelt de aanmeldende autoriteit de Commissie en de lidstaten in kennis van certificaten die moeten worden geschorst of ingetrokken;
- e) verstrekt de aanmeldende autoriteit de nationale bevoegde autoriteiten van de lidstaat waar de aanbieder zijn geregistreerde vestigingsplaats heeft, alle relevante informatie over de certificaten waarvan zij de schorsing of intrekking heeft gelast; die autoriteit neemt de gepaste maatregelen die nodig zijn om een mogelijk risico voor de gezondheid, veiligheid of grondrechten af te wenden.

8. Met uitzondering van onterecht afgegeven certificaten en indien een aanwijzing is geschorst of beperkt, blijven de certificaten geldig in een van de volgende omstandigheden:

- a) de aanmeldende autoriteit heeft binnen één maand na de schorsing of beperking bevestigd dat er met betrekking tot de certificaten waarop de schorsing of beperking van toepassing is, geen risico's voor de gezondheid, veiligheid of grondrechten bestaan, en de aanmeldende autoriteit heeft voorzien in een termijn voor maatregelen om de schorsing of beperking te ondervangen; of

- b) de anmeldende autoriteit heeft bevestigd dat er geen certificaten in verband met de schorsing zullen worden afgegeven, gewijzigd, of opnieuw afgegeven gedurende de schorsing of beperking en geeft aan of de aangemelde instantie het vermogen heeft om de bestaande, voor de periode van schorsing of beperking afgegeven certificaten te blijven monitoren en daarvoor verantwoordelijk te blijven; indien de anmeldende autoriteit vaststelt dat de aangemelde instantie niet in staat is bestaande afgegeven certificaten te ondersteunen, bevestigt de aanbieder van het systeem waarop het certificaat betrekking heeft binnen drie maanden na de schorsing of beperking aan de nationale bevoegde autoriteiten van de lidstaat waar hij zijn geregistreerde vestigingsplaats heeft via schriftelijke weg dat in plaats van de aangemelde instantie een andere gekwalificeerde aangemelde instantie tijdelijk de certificaten tijdens de periode van schorsing of beperking zal monitoren en er de verantwoordelijkheid voor zal dragen.

9. Met uitzondering van onterecht afgegeven certificaten en indien een aanwijzing is ingetrokken, blijven de certificaten in de volgende omstandigheden negen maanden geldig:

- a) de nationale bevoegde autoriteit van de lidstaat waar de aanbieder van het onder het certificaat vallende AI-systeem met een hoog risico zijn geregistreerde vestigingsplaats heeft, bevestigt heeft dat de betreffende AI-systemen met een hoog risico geen risico voor de gezondheid, veiligheid of grondrechten inhouden; en
- b) een andere aangemelde instantie schriftelijk heeft bevestigd dat zij de onmiddellijke verantwoordelijkheid voor deze AI-systemen op zich neemt en haar beoordeling binnen twaalf maanden na intrekking van de aanwijzing afrondt.

Onder de in de eerste alinea bedoelde omstandigheden kan de nationale bevoegde autoriteit van de lidstaat waarin de aanbieder van het systeem waarop het certificaat betrekking heeft, zijn vestigingsplaats heeft, de voorlopige geldigheidsduur van de certificaten verlengen met perioden van drie maanden, die samen niet meer dan twaalf maanden mogen bedragen.

De nationale bevoegde autoriteit of de aangemelde instantie die de functies van de door de wijziging van de aanwijzing getroffen aangemelde instantie vervult, stelt de Commissie, de andere lidstaten en de andere aangemelde instanties hiervan onmiddellijk in kennis.

Artikel 37

Betwisting van de bekwaamheid van aangemelde instanties

1. De Commissie onderzoekt indien nodig alle gevallen waarin er redenen zijn om te twijfelen aan de bekwaamheid van een aangemelde instantie of te twijfelen of een aangemelde instantie nog aan de eisen van artikel 31 voldoet en haar toepasselijke verantwoordelijkheden nakomt.
2. De anmeldende autoriteit verstrekt de Commissie op verzoek alle relevante informatie over de aanmelding of het op peil houden van de bekwaamheid van de betrokken aangemelde instantie.
3. De Commissie ziet erop toe dat alle gevoelige informatie die zij in de loop van haar onderzoeken op grond van dit artikel ontvangt, overeenkomstig artikel 78 vertrouwelijk wordt behandeld.

4. Wanneer de Commissie vaststelt dat een aangemelde instantie niet of niet meer aan de aanmeldingseisen voldoet, brengt zij de aanmeldende lidstaat daarvan op de hoogte en verzoekt zij deze lidstaat de nodige corrigerende maatregelen te nemen, en zo nodig de aanmelding te schorsen of in te trekken. Indien de lidstaat niet de nodige corrigerende actie onderneemt, kan de Commissie door middel van een uitvoeringshandeling de aanwijzing schorsen, beperken of intrekken. De uitvoeringshandeling wordt vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

Artikel 38

Coördinatie van aangemelde instanties

1. Ten aanzien van AI-systemen met een hoog risico zorgt de Commissie voor het instellen en naar behoren uitvoeren van passende coördinatie en samenwerking tussen aangemelde instanties die zich bezighouden met de conformiteitsbeoordelingsprocedures krachtens deze verordening in de vorm van een sectorale groep van aangemelde instanties.
2. Elke aanmeldende autoriteit zorgt ervoor dat de door haar aangemelde instanties rechtstreeks of via aangestelde vertegenwoordigers aan de werkzaamheden van een in lid 1 vermelde groep deelnemen.
3. De Commissie voorziet in de uitwisseling van kennis en beste praktijken tussen aanmeldende autoriteiten.

Artikel 39

Conformiteitsbeoordelingsinstanties van derde landen

Conformiteitsbeoordelingsinstanties die zijn opgericht naar het recht van een derde land waarmee de Unie een overeenkomst heeft gesloten, kunnen worden gemachtigd de activiteiten van aangemelde instanties krachtens deze verordening te verrichten, mits zij aan de in artikel 31 vastgelegde voorschriften voldoen of een gelijkwaardig nalevingsniveau waarborgen.

AFDELING 5

NORMEN, CONFORMITEITSBEOORDELING, CERTIFICATEN, REGISTRATIE

Artikel 40

Geharmoniseerde normen en normalisatieproducten

1. AI-systemen met een hoog risico of AI-modellen voor algemene doeleinden die in overeenstemming zijn met geharmoniseerde normen of delen daarvan, waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, overeenkomstig Verordening (EU) nr. 1025/2012, worden geacht in overeenstemming te zijn met de in afdeling 2 van dit hoofdstuk beschreven eisen, of, naargelang het geval, de in hoofdstuk V, afdelingen 2 en 3, van deze verordening beschreven verplichtingen, voor zover die eisen of verplichtingen door die normen worden gedekt.

2. Overeenkomstig artikel 10 van Verordening (EU) nr. 1025/2012 dient de Commissie zonder onnodige vertraging normalisatieverzoeken in die betrekking hebben op alle eisen van afdeling 2 van dit hoofdstuk en, in voorkomend geval, normalisatieverzoeken die betrekking hebben op verplichtingen van hoofdstuk V, afdelingen 2 en 3, van deze verordening. In het normalisatieverzoek wordt ook gevraagd om producten met betrekking tot rapporterings- en documentatieprocessen om de prestaties van hulpbronnen van AI-systemen te verbeteren, zoals het verminderen van het energieverbruik en het verbruik van andere hulpbronnen van AI-systemen met een hoog risico tijdens de levenscyclus ervan, en met betrekking tot de energie-efficiënte ontwikkeling van AI-modellen voor algemene doeleinden. Bij het opstellen van een normalisatieverzoek raadpleegt de Commissie de AI-board en de relevante belanghebbenden, met inbegrip van het adviesforum.

Bij het richten van een normalisatieverzoek aan Europese normalisatie-instellingen specificeert de Commissie dat normen duidelijk en consistent moeten zijn, met inbegrip van de normen die in de verschillende sectoren ontwikkeld zijn voor producten die onder de in bijlage I vermelde bestaande harmonisatiewetgeving van de Unie vallen, en tot doel hebben ervoor te zorgen dat AI-systemen met een hoog risico of AI-modellen voor algemene doeleinden die in de Unie in de handel worden gebracht of in gebruik worden gesteld, voldoen aan de relevante eisen of verplichtingen van deze verordening.

De Commissie verzoekt de Europese normalisatieorganisaties aan te tonen dat zij alles in het werk stellen om de in de eerste en tweede alinea van dit lid bedoelde doelstellingen te verwezenlijken overeenkomstig artikel 24 van Verordening (EU) nr. 1025/2012.

3. De deelnemers aan het normalisatieproces streven naar het bevorderen van investeringen en innovatie in AI, onder andere door voor meer rechtszekerheid te zorgen, en het concurrentievermogen en de groei van de markt van de Unie, naar het bijdragen aan de versterking van de wereldwijde samenwerking op het gebied van normalisatie, rekening houdend met bestaande internationale normen op het gebied van AI die in overeenstemming zijn met de waarden, grondrechten en belangen van de Unie, en naar het verbeteren van de multistakeholdergovernance door te zorgen voor een evenwichtige vertegenwoordiging van de belangen en de effectieve deelname van alle relevante belanghebbenden overeenkomstig de artikelen 5, 6 en 7 van Verordening (EU) nr. 1025/2012.

Artikel 41

Gemeenschappelijke specificaties

1. De Commissie kan uitvoeringshandelingen vaststellen tot vaststelling van gemeenschappelijke specificaties voor de eisen van afdeling 2 van dit hoofdstuk of, in voorkomend geval, voor de verplichtingen van hoofdstuk V, afdelingen 2 en 3, indien aan de volgende voorwaarden is voldaan:
- a) de Commissie heeft op grond van artikel 10, lid 1, van Verordening (EU) nr. 1025/2012 een of meer Europese normalisatieorganisaties verzocht een geharmoniseerde norm op te stellen voor de in afdeling 2 van dit hoofdstuk beschreven eisen, of, in voorkomend geval, voor de verplichtingen van hoofdstuk V, afdelingen 2 en 3, en:
 - i) het verzoek is door geen enkele van de Europese normalisatieorganisaties aanvaard; of

- ii) de geharmoniseerde normen waarop dat verzoek betrekking heeft, worden niet binnen de overeenkomstig artikel 10, lid 1, van Verordening (EU) nr. 1025/2012 vastgestelde termijn geleverd; of
 - iii) in de relevante geharmoniseerde normen wordt onvoldoende rekening gehouden met problemen op het gebied van de grondrechten; of
 - iv) de geharmoniseerde normen voldoen niet aan het verzoek; en
- b) er is geen referentie van geharmoniseerde normen overeenkomstig Verordening (EU) nr. 1025/2012 bekendgemaakt in het *Publicatieblad van de Europese Unie* voor de eisen van afdeling 2 van dit hoofdstuk of, in voorkomend geval, voor de verplichtingen van hoofdstuk V, afdelingen 2 en 3, en een dergelijke referentie zal naar verwachting niet binnen een redelijke termijn worden bekendgemaakt.

Bij het opstellen van de gemeenschappelijke specificaties raadpleegt de Commissie het in artikel 67 bedoelde adviesforum.

De in de eerste alinea van dit lid bedoelde uitvoeringshandelingen worden vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

2. Alvorens een ontwerpuitvoeringshandeling op te stellen, stelt de Commissie het in artikel 22 van Verordening (EU) nr. 1025/2012 bedoelde comité ervan in kennis dat zij van oordeel is dat aan de voorwaarden van lid 1 van dit artikel is voldaan.

3. AI-systemen met een hoog risico of AI-modellen voor algemene doeleinden die in overeenstemming zijn met de in lid 1 bedoelde gemeenschappelijke specificaties of delen daarvan worden geacht in overeenstemming te zijn met de in afdeling 2 van dit hoofdstuk beschreven voorschriften, of, in voorkomend geval, met de verplichtingen van hoofdstuk V, afdelingen 2 en 3, voor zover die voorschriften of die verplichtingen door die gemeenschappelijke specificaties worden bestreken.
4. Wanneer een Europese normalisatieorganisatie een geharmoniseerde norm vaststelt en deze aan de Commissie voorstelt met het oog op de bekendmaking van de referentie ervan in het *Publicatieblad van de Europese Unie*, beoordeelt de Commissie de geharmoniseerde norm overeenkomstig Verordening (EU) nr. 1025/2012. Wanneer de referentie van een geharmoniseerde norm in het *Publicatieblad van de Europese Unie* wordt bekendgemaakt, trekt de Commissie de in lid 1 bedoelde uitvoeringshandelingen of delen daarvan die dezelfde in afdeling 2 van dit hoofdstuk vermelde eisen of, in voorkomend geval, dezelfde verplichtingen van hoofdstuk V, afdelingen 2 en 3, dekken, in.
5. Wanneer aanbieders van AI-systemen met een hoog risico of AI-modellen voor algemene doeleinden niet voldoen aan de in lid 1 bedoelde gemeenschappelijke specificaties, moeten zij naar behoren rechtvaardigen dat zij technische oplossingen hebben gekozen die voldoen aan de in afdeling 2 van dit hoofdstuk beschreven voorschriften of, in voorkomend geval, aan de verplichtingen van hoofdstuk V, afdelingen 2 en 3, in een mate die minstens gelijkwaardig daarmee is.

6. Wanneer een lidstaat van oordeel is dat een gemeenschappelijke specificatie niet volledig aan de eisen van afdeling 2 van dit hoofdstuk of, in voorkomend geval, de verplichtingen van hoofdstuk V, afdelingen 2 en 3, voldoet, stelt deze lidstaat de Commissie daarvan in kennis met een gedetailleerde toelichting. De Commissie beoordeelt die informatie en wijzigt de uitvoeringshandeling tot vaststelling van de betrokken gemeenschappelijke specificatie zo nodig.

Artikel 42

Vermoeden van conformiteit met bepaalde eisen

1. AI-systemen met een hoog risico die zijn getraind en getest op data die overeenkomen met de specifieke geografische, gedragsgerelateerde, contextuele of functionele omgeving waarin zij zullen worden gebruikt, geacht te voldoen de in artikel 10, lid 4, beschreven relevante eisen.
2. AI-systemen met een hoog risico die zijn gecertificeerd of waarvoor een conformiteitsverklaring is verstrekt volgens een cyberbeveiligingsregeling krachtens Verordening (EU) 2019/881 en waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, worden geacht te voldoen aan de in artikel 15 van deze verordening beschreven cyberbeveiligingseisen, voor zover die eisen door het cyberbeveiligingscertificaat of de conformiteitsverklaring of delen daarvan worden bestreken.

Artikel 43
Conformiteitsbeoordeling

1. Voor in punt 1 van bijlage III opgesomde AI-systemen met een hoog risico kiest de aanbieder, wanneer de aanbieder bij het aantonen van de overeenstemming met de in afdeling 2 beschreven voorschriften van een AI-systeem met een hoog risico geharmoniseerde normen als bedoeld in artikel 40 of in voorkomend geval gemeenschappelijke specificaties als bedoeld in artikel 41 heeft toegepast, een van de volgende conformiteitsbeoordelingsprocedures op basis van:
 - a) de in bijlage VI bedoelde interne controle; of
 - b) de beoordeling van het systeem voor kwaliteitsbeheer en de beoordeling van de technische documentatie, met betrokkenheid van een aangemelde instantie, als bedoeld in bijlage VII.

Bij het aantonen van de overeenstemming met de in afdeling 2 beschreven voorschriften van een AI-systeem met een hoog risico volgt de aanbieder de conformiteitsbeoordelingsprocedure van bijlage VII indien:

- a) er geen geharmoniseerde normen als bedoeld in artikel 40 bestaan en er geen gemeenschappelijke specificaties als bedoeld in artikel 41 voorhanden zijn;
- b) de aanbieder de geharmoniseerde norm niet of slechts gedeeltelijk heeft toegepast;
- c) de in punt a) bedoelde gemeenschappelijke specificaties bestaan, maar de aanbieder deze niet heeft toegepast;

- d) een of meer van de in punt a) bedoelde geharmoniseerde normen met beperkingen zijn bekendgemaakt, en alleen met betrekking tot het deel van de norm waarvoor de beperkingen gelden.

Ten behoeve van de in bijlage VII bedoelde conformiteitsbeoordelingsprocedure kan de aanbieder om het even welke aangemelde instantie kiezen. Wanneer het AI-systeem met een hoog risico echter is bedoeld om door rechtshandavingsinstanties, immigratie- of asielautoriteiten of door instellingen, organen of instanties van de Unie in gebruik te worden gesteld, treedt de markttoezichtautoriteit als bedoeld in artikel 74, lid 8 of 9, naar gelang van toepassing, als aangemelde instantie op.

2. Voor AI-systemen met een hoog risico als bedoeld in de punten 2 tot en met 8 van bijlage III volgen aanbieders de in bijlage VI bedoelde conformiteitsbeoordelingsprocedure op basis van interne controled, waarvoor de betrokkenheid van een aangemelde instantie niet nodig is.
3. Voor AI-systemen met een hoog risico die onder de in afdeling A van bijlage I vermelde harmonisatiewetgeving van de Unie vallen, volgt de aanbieder de relevante conformiteitsbeoordelingsprocedure zoals vereist volgens die rechtshandelingen. De in afdeling 2 van dit hoofdstuk beschreven voorschriften zijn van toepassing op die AI-systemen met een hoog risico en maken deel uit van die beoordeling. De punten 4.3, 4.4, 4.5 en de vijfde alinea van punt 4.6 van bijlage VII zijn eveneens van toepassing.

Voor die beoordeling hebben aangemelde instanties die volgens die rechtshandelingen zijn aangemeld het recht de conformiteit van de AI-systemen met een hoog risico met de in afdeling 2 beschreven voorschriften te controleren, mits de overeenstemming van die aangemelde instanties met voorschriften van artikel 31, leden 4, 10 en 11, in de context van de aanmeldingsprocedure volgens die rechtshandelingen is beoordeeld.

Wanneer een in afdeling A van bijlage I vermelde rechtshandeling de productfabrikant in staat stelt zich te onttrekken aan een conformiteitsbeoordeling door een derde partij, mits die fabrikant alle geharmoniseerde normen voor alle relevante voorschriften heeft toegepast, kan de fabrikant alleen van die mogelijkheid gebruikmaken als hij ook geharmoniseerde normen of in voorkomend geval gemeenschappelijke specificaties als bedoeld in artikel 41 heeft toegepast, voor alle in afdeling 2 van dit hoofdstuk beschreven voorschriften.

4. AI-systemen met een hoog risico die reeds aan een conformiteitsbeoordelingsprocedure zijn onderworpen, ondergaan een nieuwe conformiteitsbeoordelingsprocedure telkens wanneer zij substantieel zijn gewijzigd, ongeacht of het gewijzigde systeem bedoeld is om verder te worden gedistribueerd of door de huidige gebruiksverantwoordelijke gebruikt blijft worden.

Voor AI-systemen met een hoog risico die doorgaan met leren na in de handel te zijn gebracht of in gebruik te zijn gesteld, vormen veranderingen van het AI-systeem met een hoog risico en de prestaties ervan die op het moment van de eerste conformiteitsbeoordeling vooraf door de aanbieder zijn bepaald en deel uitmaken van de informatie in de in punt 2, f), van bijlage IV bedoelde technische documentatie, geen substantiële wijziging.

5. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen om bijlagen VI en VII te wijzigen teneinde hen te actualiseren in het licht van technologische vooruitgang.

6. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen om de leden 1 en 2 te wijzigen, teneinde AI-systemen met een hoog risico als bedoeld in de punten 2 tot en met 8 van bijlage III te onderwerpen aan de conformiteitsbeoordelingsprocedure als bedoeld in bijlage VII of delen daarvan. De Commissie stelt zulke gedelegeerde handelingen vast rekening houdend met de doeltreffendheid van de conformiteitsbeoordelingsprocedure op basis van interne controle als bedoeld in bijlage VI bij het voorkomen of minimaliseren van de risico's voor de gezondheid en veiligheid en de bescherming van grondrechten die zulke systemen inhouden alsook met de beschikbaarheid van voldoende capaciteit en personeel onder aangemelde instanties.

Artikel 44

Certificaten

1. Door aangemelde instanties overeenkomstig bijlage VII afgegeven certificaten worden opgesteld in een taal die de desbetreffende autoriteiten in de lidstaat waar de aangemelde instantie is gevestigd, gemakkelijk kunnen begrijpen.
2. Certificaten zijn geldig gedurende de daarin aangegeven periode, die niet meer dan vijf jaar mag bedragen voor AI-systemen die onder bijlage I vallen, en niet meer dan vier jaar voor AI-systemen die onder bijlage III vallen. Op verzoek van de aanbieder kan de geldigheidsduur van een certificaat op grond van een herbeoordeling volgens de toepasselijke conformiteitsbeoordelingsprocedures worden verlengd met bijkomende perioden, die elk niet meer dan vijf jaar mogen bedragen voor AI-systemen die onder bijlage I vallen en niet meer dan vier jaar voor AI-systemen die onder bijlage III vallen. Aanvullingen op een certificaat blijven geldig zolang het certificaat dat zij aanvullen geldig blijft.

3. Indien een aangemelde instantie vaststelt dat een AI-systeem niet meer aan de in afdeling 2 beschreven voorschriften voldoet, gaat zij, rekening houdend met het evenredigheidsbeginsel, over tot schorsing of intrekking van het afgegeven certificaat of legt zij beperkingen op, tenzij de aanbieder van het systeem, met het oog op de naleving van deze voorschriften, binnen een door de aangemelde instantie vastgestelde passende termijn adequate corrigerende actie onderneemt. De aangemelde instantie geeft de redenen voor haar besluit op.

Er wordt voorzien in een beroepsprocedure tegen besluiten van de aangemelde instanties, ook inzake afgegeven conformiteitscertificaten.

Artikel 45

Informatieverplichtingen voor aangemelde instanties

1. Aangemelde instanties brengen de aanmeldende autoriteit op de hoogte van:
- a) beoordelingscertificaten van technische documentatie van de Unie, aanvullingen op die certificaten en goedkeuringen voor systemen voor kwaliteitsbeheer afgegeven overeenkomstig de eisen van bijlage VII;
 - b) weigering, beperking, schorsing of intrekking van een beoordelingscertificaat technische documentatie van de Unie of een goedkeuring voor systemen voor kwaliteitsbeheer afgegeven overeenkomstig de eisen van bijlage VII;
 - c) omstandigheden die van invloed zijn op het toepassingsgebied van of de voorwaarden voor de aanmelding;

- d) verzoeken om informatie over conformiteitsbeoordelingsactiviteiten die zij van markttoezichtautoriteiten ontvangen;
 - e) op verzoek, de binnen het toepassingsgebied van hun aanmelding verrichte conformiteitsbeoordelingsactiviteiten en andere activiteiten, waaronder grensoverschrijdende activiteiten en onderaanneming.
2. Elke aangemelde instantie brengt de andere aangemelde instanties op de hoogte van:
- a) door haar geweigerde, opgeschorte of ingetrokken goedkeuringen voor kwaliteitsbeheersystemen alsmede, op verzoek, van de door haar verleende goedkeuringen voor systemen voor kwaliteitsbeheer;
 - b) beoordelingscertificaten van technische documentatie van de Unie of aanvullingen daarop die zij heeft geweigerd, ingetrokken, opgeschort of anderszins beperkt alsmede, op verzoek, de certificaten en/of aanvullingen daarop die zij heeft uitgegeven.
3. Elke aangemelde instantie verstrekt de andere aangemelde instanties die soortgelijke conformiteitsbeoordelingsactiviteiten voor dezelfde soorten AI-systemen verrichten, relevante informatie over negatieve conformiteitsbeoordelingsresultaten, en op verzoek ook over positieve conformiteitsbeoordelingsresultaten.
4. Aanmeldende autoriteiten waarborgen dat de door hen verkregen informatie overeenkomstig artikel 78 vertrouwelijk wordt behandeld.

Artikel 46

Afwijking van de conformiteitsbeoordelingsprocedure

1. In afwijking van artikel 43 en op naar behoren gemotiveerd verzoek kan een markttoezichtautoriteit het in de handel brengen of het in gebruik stellen van specifieke AI-systemen met een hoog risico binnen het grondgebied van de betrokken lidstaat toelaten, om uitzonderlijke redenen van openbare veiligheid of de bescherming van het leven en de gezondheid van personen, milieubescherming of de bescherming van essentiële industriële en infrastructurele activa. De toelating geldt gedurende een beperkte periode, terwijl de nodige conformiteitsbeoordelingsprocedures worden uitgevoerd, rekening houdend met de uitzonderlijke redenen ter rechtvaardiging van de afwijking. Die procedures worden zo snel mogelijk afgerond.
2. In een naar behoren gerechtvaardigde situatie van urgentie om uitzonderlijke redenen van openbare veiligheid of in geval van een specifieke, substantiële en imminente dreiging voor het leven of de fysieke veiligheid van natuurlijke personen, kunnen rechtshandavingsinstanties of civielebeschermingsautoriteiten een specifiek AI-systeem met een hoog risico in gebruik stellen zonder de in lid 1 bedoelde toelating, op voorwaarde dat die toelating tijdens of na het gebruik zonder onnodige vertraging wordt aangevraagd. Indien de in lid 1 bedoelde toelating wordt geweigerd, wordt het gebruik van het AI-systeem met een hoog risico met onmiddellijke ingang stopgezet en worden alle resultaten en outputs van dat gebruik onmiddellijk verwijderd.

3. De in lid 1 bedoelde toelating wordt alleen verstrekt als de markttoezichtautoriteit concludeert dat het AI-systeem met een hoog risico aan de voorschriften van afdeling 2 voldoet. De markttoezichtautoriteit stelt de Commissie en de andere lidstaten in kennis van op grond van de leden 1 en 2 verstrekte toelatingen. Deze verplichting geldt niet voor gevoelige operationele gegevens met betrekking tot de activiteiten van rechtshandavingsinstanties.
4. Indien binnen 15 kalenderdagen na de ontvangst van de in lid 3 bedoelde informatie geen bezwaar is geopperd door een lidstaat of de Commissie tegen een door een markttoezichtautoriteit van een lidstaat overeenkomstig lid 1 verstrekte toelating, wordt die toelating geacht gerechtvaardigd te zijn.
5. Indien binnen 15 kalenderdagen na de ontvangst van in lid 3 bedoelde kennisgeving door een lidstaat bezwaren worden geopperd tegen een door een markttoezichtautoriteit van een andere lidstaat verstrekte toelating, of wanneer de Commissie de toelating in strijd met het Unierecht acht of de conclusie van de lidstaten ten aanzien van de conformiteit van het systeem als bedoeld in lid 3 ongegrond acht, treedt de Commissie onverwijld in overleg met de relevante lidstaat. De betrokken operatoren worden geraadpleegd en hebben de mogelijkheid hun standpunten uiteen te zetten. Met het oog daarop besluit de Commissie of de toelating gerechtvaardigd is. De Commissie richt haar besluit aan de betrokken lidstaat en de relevante operatoren.
6. Indien de Commissie de toelating ongerechtvaardigd acht, wordt deze ingetrokken door de markttoezichtautoriteit van de betrokken lidstaat.

7. Voor AI-systemen met een hoog risico die verband houden met producten die onder de in afdeling A van bijlage I vermelde harmonisatiewetgeving van de Unie vallen, zijn alleen de in die harmonisatiewetgeving van de Unie vastgestelde afwijkingen van de conformiteitsbeoordeling van toepassing.

Artikel 47

EU-conformiteitsverklaring

1. De aanbieder stelt voor elk AI-systeem met een hoog risico een schriftelijke machineleesbare, fysieke of elektronisch ondertekende EU-conformiteitsverklaring op en houdt deze verklaring tot tien jaar na het in de handel brengen of het in gebruik stellen van het AI-systeem met een hoog risico ter beschikking van de nationale bevoegde autoriteiten. In de EU-conformiteitsverklaring wordt vermeld voor welk AI-systeem met een hoog risico ze is opgesteld. Op verzoek wordt een kopie van de EU-conformiteitsverklaring aan de relevante nationale bevoegde autoriteiten voorgelegd.
2. In de EU-conformiteitsverklaring wordt vermeld dat het betreffende AI-systeem met een hoog risico aan de in afdeling 2 beschreven voorschriften voldoet. De EU-conformiteitsverklaring bevat de informatie die is vervat in bijlage V en wordt vertaald in een taal die de nationale bevoegde autoriteiten van de lidstaten waarin het AI-systeem met een hoog risico in de handel wordt gebracht of wordt aangeboden, gemakkelijk kunnen begrijpen.

3. Wanneer AI-systemen met een hoog risico onder andere harmonisatiewetgeving van de Unie vallen, waarvoor ook een EU-conformiteitsverklaring is vereist, wordt één EU-conformiteitsverklaring ten aanzien van alle op het AI-systeem met een hoog risico toepasselijke Uniewetgeving opgesteld. De verklaring bevat alle informatie die vereist is voor de identificatie van de harmonisatiewetgeving van de Unie waarop de verklaring betrekking heeft.
4. Met het opstellen van de EU-conformiteitsverklaring neemt de aanbieder de verantwoordelijkheid op zich om de in afdeling 2 beschreven voorschriften na te leven. De aanbieder houdt de EU-conformiteitsverklaring voor zover dienstig up-to-date.
5. De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen om bijlage V te wijzigen door het actualiseren van de in die bijlage beschreven inhoud van de EU-conformiteitsverklaring, teneinde elementen in te voeren die noodzakelijk worden in het licht van de technische vooruitgang.

Artikel 48

CE-markering

1. De CE-markering is onderworpen aan de algemene beginselen die zijn neergelegd in artikel 30 van Verordening (EG) nr. 765/2008.
2. Voor digitaal aangeboden AI-systemen met een hoog risico wordt alleen een digitale CE-markering gebruikt als deze gemakkelijk toegankelijk is via de interface waarmee toegang wordt verkregen tot dat systeem of via een gemakkelijk toegankelijke machineleesbare code of andere elektronische middelen.

3. De CE-markering wordt zichtbaar, leesbaar en onuitwisbaar op AI-systemen met een hoog risico aangebracht. Wanneer dit gezien de aard van het AI-systeem met een hoog risico niet mogelijk of niet gerechtvaardigd is, wordt de markering naargelang het geval op de verpakking of in de begeleidende documenten aangebracht.
4. Indien van toepassing, wordt de CE-markering gevolgd door het identificatienummer van de aangemelde instantie die verantwoordelijk is voor de in artikel 43 beschreven conformiteitsbeoordelingsprocedures. Het identificatienummer van de aangemelde instantie wordt aangebracht door die instantie zelf dan wel overeenkomstig haar instructies door de aanbieder of door diens gemachtigde. Het identificatienummer wordt ook vermeld in reclamemateriaal waarin staat dat een AI-systeem met een hoog risico aan de eisen voor de CE-markering voldoet.
5. Indien AI-systemen met een hoog risico onder andere Uniewetgeving vallen die ook betrekking heeft op het aanbrengen van de CE-markering, vermeldt de CE-markering dat de AI-systemen met een hoog risico tevens aan de voorschriften van die andere wetgeving voldoen.

Artikel 49

Registratie

1. Alvorens een in bijlage III vermeld AI-systeem met een hoog risico, met uitzondering van de in punt 2 van bijlage III vermelde AI-systemen met een hoog risico, in de handel te brengen of in gebruik te stellen, registreert de aanbieder of in voorkomend geval de gemachtigde zichzelf en zijn systeem in de in artikel 71 bedoelde EU-databank.

2. Alvorens een AI-systeem in de handel te brengen of in gebruik te stellen dat naar oordeel van de aanbieder geen hoog risico inhoudt volgens artikel 6, lid 3, registreert die aanbieder of in voorkomend geval de gemachtigde zichzelf en dat systeem in de in artikel 71 bedoelde EU-databank.
3. Alvorens een in bijlage III vermeld AI-systeem met een hoog risico in gebruik te stellen of te gebruiken, met uitzondering van de in punt 2 van bijlage III vermelde AI-systemen met een hoog risico, registreren gebruiksverantwoordelijken die overheidsinstanties, instellingen, organen of instanties van de Unie, of personen die namens hen optreden, zichzelf en selecteren zij het systeem en registreren zij het gebruik ervan in de in artikel 71 bedoelde EU-databank.
4. Voor AI-systemen met een hoog risico als bedoeld in de punten 1, 6 en 7 van bijlage III, op het gebied van rechtshandhaving, migratie, asiel en grenstoezichtsbeheer, vindt de in de leden 1, 2 en 3 van dit artikel bedoelde registratie plaats in een beveiligd niet-openbaar gedeelte van de in artikel 71 bedoelde EU-databank en bevat deze alleen de volgende informatie, voor zover van toepassing, als bedoeld in:
 - a) afdeling A, punten 1 tot en met 10, van bijlage VIII, met uitzondering van punten 6, 8 en 9;
 - b) afdeling B, punten 1 tot en met 5, en punten 8 en 9 van bijlage VIII;
 - c) afdeling C, punten 1 tot en met 3, van bijlage VIII;
 - d) de punten 1, 2, 3 en 5 van bijlage IX.

Alleen de Commissie en de in artikel 74, lid 8, bedoelde nationale autoriteiten hebben toegang tot de respectieve in de eerste alinea van dit lid vermelde beperkt toegankelijke gedeelten van de EU-databank.

5. AI-systemen met een hoog risico als bedoeld in punt 2 van bijlage III worden op nationaal niveau geregistreerd.

Hoofdstuk IV

Transparantieverplichtingen voor aanbieders en gebruiksverantwoordelijken van bepaalde AI-systemen

Artikel 50

Transparantieverplichtingen voor aanbieders en gebruiksverantwoordelijken van bepaalde AI-systemen

1. Aanbieders zorgen ervoor dat AI-systemen die voor directe interactie met natuurlijke personen zijn bedoeld, zodanig worden ontworpen en ontwikkeld dat de betrokken natuurlijke personen worden geïnformeerd dat zij interageren met een AI-systeem, tenzij dit duidelijk is vanuit het oogpunt van een normaal geïnformeerde en redelijk omzichtige en oplettende natuurlijke persoon, rekening houdend met de omstandigheden en de gebruikscontext. Deze verplichting is niet van toepassing op bij wet toegestane AI-systemen voor het opsporen, voorkomen, onderzoeken of vervolgen van strafbare feiten, met inachtneming van passende waarborgen voor de rechten en vrijheden van derden, tenzij die systemen voor het publiek beschikbaar zijn om een strafbaar feit te melden.

2. Aanbieders van AI-systemen, met inbegrip van AI-systemen voor algemene doeleinden, die synthetische audio-, beeld-, video- of tekstinhoud genereren, zorgen ervoor dat de outputs van het AI-systeem worden gemarkeerd in een machineleesbaar formaat en detecteerbaar zijn als kunstmatig gegenereerd of gemanipuleerd. Aanbieders zorgen ervoor dat hun technische oplossingen doeltreffend, interoperabel, robuust en betrouwbaar zijn voor zover dat technisch haalbaar is, rekening houdend met de specifieke kenmerken en beperkingen van de verschillende soorten content, de uitvoeringskosten en de algemeen erkende stand van de techniek, zoals tot uiting kan komen in relevante technische normen. Deze verplichting is niet van toepassing voor zover de AI-systemen een ondersteunende functie voor standaardbewerking vervullen of de door de gebruiksverantwoordelijke of de semantiek daarvan verstrekte inputdata niet substantieel wijzigen, of wanneer het bij wet is toegestaan strafbare feiten op te sporen, te voorkomen, te onderzoeken of te vervolgen.
3. Gebruiksverantwoordelijken van een systeem voor het herkennen van emoties of een systeem voor biometrische categorisering informeren de daaraan blootgestelde natuurlijke personen over de werking van het systeem en verwerken de persoonsgegevens in overeenstemming met Verordening (EU) 2016/679, Verordening (EU) 2018/1725 en Richtlijn (EU) 2016/680, indien van toepassing. Deze verplichting is niet van toepassing op voor biometrische categorisering en emotieherkenning gebruikte AI-systemen, die bij wet zijn toegestaan om strafbare feiten op te sporen, te voorkomen of te onderzoeken, met inachtneming van passende waarborgen voor de rechten en vrijheden van derden en overeenkomstig het Unierecht.

4. Gebruiksverantwoordelijken van een AI-systeem dat beeld-, audio- of videocontent genereert of bewerkt die een deepfake vormt, maken bekend dat de content kunstmatig is gegenereerd of gemanipuleerd. Deze verplichting geldt niet wanneer het gebruik bij wet is toegestaan om strafbare feiten op te sporen, te voorkomen, te onderzoeken of te vervolgen. Wanneer de content deel uitmaakt van een kennelijk artistiek, creatief, satirisch, fictief of analoog werk of programma, zijn de transparantieplichtingen van dit lid beperkt tot de openbaarmaking van het bestaan van dergelijke gegenereerde of bewerkte content op een passende wijze die de weergave of het genot van het werk niet belemmert.

Gebruiksverantwoordelijken van een AI-systeem dat tekst genereert of bewerkt die wordt gepubliceerd om het publiek te informeren over aangelegenheden van algemeen belang, maken bekend dat de tekst kunstmatig is gegenereerd of bewerkt. Deze verplichting is echter niet van toepassing wanneer het gebruik bij wet is toegestaan om strafbare feiten op te sporen, te voorkomen, te onderzoeken of te vervolgen of wanneer de door AI gegenereerde content een proces van menselijke toetsing of redactionele controle heeft ondergaan en wanneer een natuurlijke of rechtspersoon redactionele verantwoordelijkheid draagt voor de bekendmaking van de content.

5. De in de leden 1 tot en met 4 bedoelde informatie wordt uiterlijk op het moment van de eerste interactie of blootstelling op duidelijke en te onderscheiden wijze aan de betrokken natuurlijke personen verstrekt. De informatie moet aan de toepasselijke toegankelijkheidseisen voldoen.
6. De leden 1 tot en met 4 laten de voorschriften en verplichtingen van hoofdstuk III onverlet en doen geen afbreuk aan andere transparantieplichtingen die zijn vastgelegd in het Unierecht of het nationale recht voor gebruiksverantwoordelijken van AI-systemen.

7. Het AI-bureau stimuleert en faciliteert de opstelling van praktijkcodes op het niveau van de Unie om de doeltreffende uitvoering van de verplichtingen met betrekking tot de opsporing en het labelen van kunstmatig gegenereerde of bewerkte content te vergemakkelijken. De Commissie kan uitvoeringshandelingen vaststellen om die praktijkcodes overeenkomstig de procedure van artikel 56, lid 6, goed te keuren. Indien zij de code ontoereikend acht, kan de Commissie volgens de onderzoeksprocedure van artikel 98, lid 2, een uitvoeringshandeling vaststellen waarin gemeenschappelijke regels voor de uitvoering van die verplichtingen worden gespecificeerd.

Hoofdstuk V

AI-modellen voor algemene doeleinden

AFDELING 1

CLASSIFICATIEREGELS

Artikel 51

Classificatie van AI-modellen voor algemene doeleinden

als AI-modellen voor algemene doeleinden met een systeemrisico

1. Een AI-model voor algemene doeleinden wordt geclassificeerd als een AI-model voor algemene doeleinden met een systeemrisico als het aan één van de volgende voorwaarden voldoet:
 - a) het beschikt over capaciteiten met een grote impact die worden geëvalueerd op basis van passende technische instrumenten en methoden, met inbegrip van indicatoren en benchmarks;

- b) op grond van een besluit van de Commissie, ambtshalve of naar aanleiding van een gekwalificeerde waarschuwing van het wetenschappelijk panel, heeft het AI-model vergelijkbare capaciteiten of een vergelijkbare impact als beschreven in punt a), met inachtneming van de criteria in bijlage XIII.
2. Een AI-model voor algemene doeleinden wordt geacht capaciteiten met een grote impact overeenkomstig lid 1, punt a), te hebben wanneer de cumulatieve hoeveelheid berekeningen die wordt gebruikt om het model te trainen, gemeten in zwevendekomma bewerkingen, groter is dan 10^{25} .
3. De Commissie stelt overeenkomstig artikel 97 gedelegeerde handelingen vast om de in de leden 1 en 2 van dit artikel genoemde drempelwaarden te wijzigen en benchmarks en indicatoren zo nodig aan te vullen in het licht van veranderende technologische ontwikkelingen, zoals algoritmische verbeteringen of verhoogde efficiëntie van de hardware, zodat deze drempels de stand van de techniek weerspiegelen.

Artikel 52

Procedure

1. Indien een AI-model voor algemene doeleinden voldoet aan de in artikel 51, lid 1, punt a), bedoelde voorwaarde, stelt de betrokken aanbieder de Commissie daarvan onverwijld in kennis, doch in ieder geval binnen twee weken nadat aan die eis is voldaan of nadat bekend is geworden dat aan die eis zal worden voldaan. Die kennisgeving bevat de informatie die nodig is om aan te tonen dat aan de desbetreffende eis is voldaan. Als de Commissie kennis krijgt van een AI-model voor algemene doeleinden dat systeemrisico's vertoont waarvan zij niet in kennis is gesteld, kan zij besluiten dit model aan te wijzen als een model met een systeemrisico.

2. De aanbieder van een AI-model voor algemene doeleinden dat voldoet aan de in artikel 51, lid 1, punt a), bedoelde voorwaarden, kan bij zijn kennisgeving voldoende onderbouwde argumenten aanvoeren om aan te tonen dat het AI-model voor algemene doeleinden, hoewel het voldoet aan die eis, bij wijze van uitzondering, vanwege zijn specifieke kenmerken geen systeemrisico's vertoont en derhalve niet zou mogen worden geclassificeerd als een AI-model voor algemene doeleinden met een systeemrisico.
3. Indien de Commissie concludeert dat de uit hoofde van lid 2 aangevoerde argumenten niet voldoende onderbouwd zijn en de desbetreffende aanbieder niet kan aantonen dat het AI-model voor algemene doeleinden vanwege zijn specifieke kenmerken geen systeemrisico's vertoont, verwerpt zij deze argumenten en wordt het AI-model voor algemene doeleinden beschouwd als een AI-model voor algemene doeleinden met een systeemrisico.
4. De Commissie kan ambtshalve of na een gekwalificeerde waarschuwing van het wetenschappelijk panel op grond van artikel 90, lid 1, punt a), op basis van de in bijlage XIII vastgestelde criteria een AI-model voor algemene doeleinden aanwijzen als een AI-model dat systeemrisico's vertoont.

De Commissie is bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen om bijlage XIII te wijzigen door de in die bijlage beschreven criteria te specificeren en te actualiseren.

5. Als een aanbieder wiens model op grond van lid 4 is aangewezen als AI-model voor algemene doeleinden met een systeemrisico een met redenen omkleed verzoek indient, neemt de Commissie dit in overweging en kan zij besluiten om opnieuw te beoordelen of het AI-model voor algemene doeleinden op basis van de criteria van bijlage XIII nog steeds wordt beschouwd als een AI-model dat systeemrisico's vertoont. Een dergelijk verzoek moet objectieve, gedetailleerde en nieuwe redenen bevatten die na het aanwijzingsbesluit aan het licht zijn gekomen. Aanbieders kunnen ten vroegste zes maanden na het aanwijzingsbesluit om een herbeoordeling verzoeken. Indien de Commissie na haar herbeoordeling besluit de aanwijzing als AI-model voor algemene doeleinden met een systeemrisico te handhaven, kunnen aanbieders pas na zes maanden na dat besluit opnieuw om een herbeoordeling verzoeken.
6. De Commissie zorgt ervoor dat er een lijst met AI-modellen voor algemene doeleinden met een systeemrisico wordt gepubliceerd en houdt die lijst actueel, onverminderd de noodzaak om intellectuele-eigendomsrechten en vertrouwelijke bedrijfsinformatie of bedrijfsgeheimen te eerbiedigen en te beschermen overeenkomstig het Unierecht en het nationale recht.

AFDELING 2
VERPLICHTINGEN VOOR AANBIEDERS VAN
AI-MODELLEN VOOR ALGEMENE DOELEINDEN

Artikel 53

Verplichtingen voor aanbieders van AI-modellen voor algemene doeleinden

1. Aanbieders van AI-modellen voor algemene doeleinden moeten:
 - a) de technische documentatie van het model opstellen en up-to-date houden, inclusief het trainings- en testproces en de resultaten van de evaluatie ervan, die ten minste de in bijlage XI vermelde informatie moet bevatten, zodat deze op verzoek aan het AI-bureau en de nationale bevoegde autoriteiten kunnen worden verstrekt;
 - b) informatie en documentatie opstellen, up-to-date houden en beschikbaar stellen voor aanbieders van AI-systemen die het AI-model voor algemene doeleinden in hun AI-systemen willen integreren. Onverminderd de noodzaak om intellectuele-eigendomsrechten en vertrouwelijke bedrijfsinformatie of bedrijfsgeheimen overeenkomstig het Unierecht en het nationale recht te eerbiedigen en te beschermen, moet de informatie en documentatie:
 - i) aanbieders van AI-systemen inzicht geven in de capaciteiten en beperkingen van het AI-model voor algemene doeleinden en ze in staat te stellen aan hun verplichtingen uit hoofde van deze verordening te voldoen; en
 - ii) ten minste de in bijlage XII uiteengezette elementen bevatten;

- c) beleid opstellen ter naleving van het Unierecht inzake auteursrechten en naburige rechten en dan met name ter vaststelling en naleving, onder meer door middel van geavanceerde technologieën, van een op grond van artikel 4, lid 3, van Richtlijn (EU) 2019/790 tot uitdrukking gebracht voorbehoud van rechten.
 - d) een voldoende gedetailleerde samenvatting opstellen en openbaar maken over de voor het trainen van het AI-model voor algemene doeleinden gebruikte content, volgens een door het AI-bureau verstrekt sjabloon.
2. De in lid 1, punten a) en b) genoemde verplichtingen gelden niet voor aanbieders van AI-modellen die worden vrijgegeven in het kader van een vrije en opensource licentie die de raadpleging, het gebruik, de wijziging en distributie van het model mogelijk maakt en waarvan de parameters, met inbegrip van de wegingen, de informatie over de modelarchitectuur en de informatie over het gebruik van het model, openbaar worden gemaakt. Deze uitzondering is niet van toepassing op AI-modellen voor algemene doeleinden met systeemrisico's.
3. Aanbieders van AI-modellen voor algemene doeleinden werken zo nodig samen met de Commissie en de nationale bevoegde autoriteiten bij de uitoefening van hun bevoegdheden uit hoofde van deze verordening.

4. Aanbieders van AI-modellen voor algemene doeleinden kunnen zich baseren op praktijkcodes in de zin van artikel 56 om de naleving van de in lid 1 van dit artikel vastgestelde verplichtingen aan te tonen, totdat er een geharmoniseerde norm is gepubliceerd. Door Europese geharmoniseerde normen na te leven genieten aanbieders een vermoeden van overeenstemming, voor zover die normen die verplichtingen dekken. Aanbieders van AI-modellen voor algemene doeleinden die zich niet aan een goedgekeurde praktijkcode houden of niet voldoen aan een Europese geharmoniseerde norm, tonen alternatieve passende wijzen van naleving aan die door de Commissie moeten worden beoordeeld.
5. Om de naleving van bijlage XI, en met name de punten 2 d) en 2 e), te vergemakkelijken, is de Commissie bevoegd overeenkomstig artikel 97 gedelegeerde handelingen vast te stellen waarin de meet- en berekeningsmethoden worden gespecificeerd zodat de documentatie vergelijkbaar en verifieerbaar wordt.
6. De Commissie is bevoegd overeenkomstig artikel 97, lid 2, gedelegeerde handelingen vast te stellen om bijlagen XI en XII te wijzigen in het licht van evoluerende technologische ontwikkelingen.
7. Uit hoofde van dit artikel verkregen informatie of documentatie, met inbegrip van bedrijfsgeheimen, worden verwerkt overeenkomstig de in artikel 78 vastgelegde vertrouwelijkheidsverplichtingen.

Artikel 54

Gemachtigden van aanbieders van AI-modellen voor algemene doeleinden

1. Aanbieders die in derde landen zijn gevestigd, wijzen voordat zij een AI-model voor algemene doeleinden in de Unie in de handel brengen, middels een schriftelijke machtiging een gemachtigde aan die is gevestigd in de Unie.

2. De aanbieder stelt zijn gemachtigde in staat de taken uit te voeren die staan gespecificeerd in het mandaat dat hij van de aanbieder heeft ontvangen.
3. De gemachtigde voert de taken uit die staan gespecificeerd in het mandaat dat hij van de aanbieder heeft ontvangen. Hij legt op verzoek een kopie van het mandaat over aan het AI-bureau, in een van de officiële talen van de instellingen van de Unie. Voor de toepassing van deze verordening geeft het mandaat de gemachtigde de bevoegdheid om de volgende taken te verrichten:
 - a) controleren of de aanbieder de in bijlage XI gespecificeerde technische documentatie heeft opgesteld en aan alle in artikel 53 en, indien van toepassing, artikel 55 bedoelde verplichtingen heeft voldaan;
 - b) een kopie van de in bijlage XI gespecificeerde technische documentatie beschikbaar houden voor het AI-bureau en de nationale autoriteiten gedurende een periode van tien jaar nadat het AI-model voor algemene doeleinden in de handel is gebracht, en de contactgegevens van de aanbieder door wie de gemachtigde is aangewezen;
 - c) het verstrekken aan het AI-bureau, na een met redenen omkleed verzoek, van alle informatie en documentatie, waaronder die in punt b), die nodig is om aan te tonen dat de verplichtingen van dit hoofdstuk worden nageleefd;
 - d) samenwerken met het AI-bureau en de bevoegde autoriteiten, na een met redenen omkleed verzoek, bij alle maatregelen die de autoriteiten nemen in verband met het AI-model voor algemene doeleinden, ook indien het model wordt geïntegreerd in AI-systemen die in de Unie in de handel worden gebracht of in gebruik worden gesteld.

4. Door het mandaat wordt de gemachtigde aangesteld als aanspreekpunt, naast of in plaats van de aanbieder, voor het AI-bureau of de bevoegde autoriteiten, met betrekking tot alle vraagstukken die verband houden met het waarborgen van de naleving van deze verordening.
5. De gemachtigde beëindigt het mandaat indien hij van mening is of redenen heeft om aan te nemen dat de aanbieder in strijd met zijn verplichtingen op grond van deze verordening handelt. In dat geval stelt hij tevens het AI-bureau onmiddellijk in kennis van de beëindiging van het mandaat en de redenen daarvoor.
6. De in dit artikel genoemde verplichting geldt niet voor aanbieders van AI-modellen die worden vrijgegeven in het kader van een vrije en opensource licentie die de raadpleging, het gebruik, de wijziging en distributie van het model mogelijk maakt en waarvan de parameters, met inbegrip van de wegingen, de informatie over de modelarchitectuur en de informatie over het gebruik van het model, openbaar worden gemaakt, tenzij de AI-modellen voor algemene doeleinden systeemrisico's vertonen.

AFDELING 3
VERPLICHTINGEN VAN AANBIEDERS VAN AI-MODELLEN
VOOR ALGEMENE DOELEINDEN MET EEN SYSTEEMRISICO

Artikel 55

*Verplichtingen van aanbieders van AI-modellen
voor algemene doeleinden met een systeemrisico*

1. Naast de in de artikelen 53 en 54 genoemde verplichtingen moeten aanbieders van AI-modellen voor algemene doeleinden met een systeemrisico:
 - a) een modevaluatie uitvoeren overeenkomstig gestandaardiseerde protocollen en instrumenten die de stand van de techniek weerspiegelen, met inbegrip van het uitvoeren en documenteren van tests gericht op het ontdekken van kwetsbaarheden van het model met als doel om systeemrisico's in kaart te brengen en te beperken;
 - b) mogelijke systeemrisico's op Unieniveau beoordelen en beperken, met inbegrip van de bronnen daarvan, die kunnen voortvloeien uit de ontwikkeling, het in de handel brengen of het gebruik van AI-modellen voor algemene doeleinden met een systeemrisico;
 - c) relevante informatie over ernstige incidenten en mogelijke corrigerende maatregelen bijhouden, documenteren en onverwijld rapporteren aan het AI-bureau en, in voorkomend geval, aan de nationale bevoegde autoriteiten;
 - d) zorgen voor een passend niveau van cyberbeveiligingsbescherming voor het AI-model voor algemene doeleinden met een systeemrisico en de fysieke infrastructuur van het model.

2. Aanbieders van AI-modellen voor algemene doeleinden met een systeemrisico kunnen zich baseren op praktijkcodes in de zin van artikel 56 om de naleving van de in lid 1 van dit artikel vastgestelde verplichtingen aan te tonen, totdat er een geharmoniseerde norm is gepubliceerd. Door Europese geharmoniseerde normen na te leven genieten aanbieders een vermoeden van overeenstemming, voor zover die normen ook die verplichtingen dekken. Aanbieders van AI-modellen voor algemene doeleinden met een systeemrisico die zich niet aan een goedgekeurde praktijkcode houden of niet voldoen aan een Europese geharmoniseerde norm, tonen alternatieve passende wijzen van naleving aan die door de Commissie moeten worden beoordeeld.
3. Uit hoofde van dit artikel verkregen informatie of documentatie, met inbegrip van bedrijfsgeheimen, worden verwerkt overeenkomstig de in artikel 78 vastgelegde vertrouwelijkheidsverplichtingen.

AFDELING 4

PRAKTIJKCODES

Artikel 56

Praktijkcodes

1. Het AI-bureau stimuleert en faciliteert de opstelling van praktijkcodes op Unieniveau als bijdrage aan de correcte toepassing van deze verordening, rekening houdend met internationale benaderingen.

2. Het AI-bureau en de AI-board streven ernaar ervoor te zorgen dat de praktijkcodes ten minste de verplichtingen omvatten die zijn bepaald in de artikelen 53 en 55, waaronder de volgende zaken:
- a) de middelen om ervoor te zorgen dat de in artikel 53, lid 1, punten a) en b), bedoelde informatie up-to-date wordt gehouden in het licht van markt- en technologische ontwikkelingen;
 - b) de mate van gedetailleerdheid van de samenvatting over de voor het trainen van het AI-model gebruikte content;
 - c) het in kaart brengen van het type en de aard van de systeemrisico's op Unieniveau, met inbegrip van de bronnen ervan, indien van toepassing;
 - d) de maatregelen, procedures en modaliteiten voor de beoordeling en het beheer van de systeemrisico's op Unieniveau, met inbegrip van de documentatie daarvan, die in verhouding moeten staan tot de risico's, rekening houden met de ernst en waarschijnlijkheid ervan en met de specifieke uitdagingen om die risico's aan te pakken in het licht van de mogelijke manieren waarop dergelijke risico's in de AI-waardeketen kunnen ontstaan en zich voordoen.
3. Het AI-bureau kan alle aanbieders van AI-modellen voor algemene doeleinden en relevante nationale bevoegde autoriteiten uitnodigen om deel te nemen aan het opstellen van praktijkcodes. Maatschappelijke organisaties, het bedrijfsleven, de academische wereld en andere relevante belanghebbenden, zoals aanbieders verder in de AI-waardeketen en onafhankelijke deskundigen, kunnen het proces ondersteunen.

4. Het AI-bureau en de AI-board streven ernaar ervoor te zorgen dat hun specifieke doelstellingen in de praktijkcodes duidelijk uiteen worden gezet en toezeggingen of maatregelen bevatten, met inbegrip van, waar passend, kernprestatie-indicatoren, om ervoor te zorgen dat die doelstellingen worden verwezenlijkt, en dat de praktijkcodes naar behoren rekening houden met de behoeften en belangen van alle belanghebbenden, met inbegrip van betrokken personen, op Unieniveau.
5. Het AI-bureau streeft ernaar ervoor te zorgen dat de deelnemers aan de praktijkcodes regelmatig verslag uitbrengen aan het AI-bureau over de uitvoering van de verbintenissen en de genomen maatregelen en de resultaten daarvan, onder meer waar nodig gemeten aan de hand van de kernprestatie-indicatoren. De kernprestatie-indicatoren en rapportageverplichtingen weerspiegelen de verschillen in omvang en capaciteit tussen de verschillende deelnemers.
6. Het AI-bureau en de AI-board monitoren en evalueren regelmatig of de deelnemers de doelstellingen van de praktijkcodes verwezenlijken en bijdragen aan de correcte toepassing van deze verordening. Het AI-bureau en de AI-board beoordelen of de praktijkcodes betrekking hebben op de verplichtingen van de artikelen 53 en 55, en monitoren en evalueren regelmatig of de doelstellingen daarvan worden verwezenlijkt. Zij maken hun beoordeling of de praktijkcodes toereikend zijn bekend.

De Commissie kan door middel van een uitvoeringshandeling een praktijkcode goedkeuren en deze binnen de Unie een algemene geldigheid verlenen. Die uitvoeringshandeling wordt vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

7. Het AI-bureau kan alle aanbieders van AI-modellen voor algemene doeleinden uitnodigen zich aan de praktijkcodes te houden. Voor aanbieders van AI-modellen voor algemene doeleinden die geen systeemrisico's inhouden, kan deze naleving worden beperkt tot de verplichtingen van artikel 53, tenzij zij uitdrukkelijk verklaren dat zij belangstelling hebben om zich bij de volledige code aan te sluiten.
8. Het AI-bureau stimuleert en faciliteert in voorkomend geval ook de evaluatie en aanpassing van de praktijkcodes, met name wanneer er nieuwe normen worden ingesteld. Het AI-bureau helpt bij de beoordeling van de beschikbare normen.
9. De praktijkcodes moeten uiterlijk op ... [negen maanden na de datum van inwerkingtreding van deze verordening] gereed zijn. Het AI-bureau neemt de nodige stappen, met inbegrip van het uitnodigen van aanbieders op grond van lid 7.

Als er uiterlijk op ... [12 maanden na de datum van inwerkingtreding] nog geen praktijkcode tot stand is gebracht, of indien het AI-bureau deze na zijn beoordeling uit hoofde van lid 6 van dit artikel ontoereikend acht, kan de Commissie door middel van uitvoeringshandelingen gemeenschappelijke regels vaststellen voor de uitvoering van de verplichtingen waarin de artikelen 53 en 55 voorzien, met inbegrip van de in lid 2 van dit artikel genoemde zaken. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

Hoofdstuk VI

Maatregelen ter ondersteuning van innovatie

Artikel 57

AI-testomgevingen voor regelgeving

1. De lidstaten zorgen ervoor dat hun bevoegde autoriteiten ten minste één AI-testomgeving voor regelgeving op nationaal niveau opzetten, die uiterlijk op ... [24 maanden na de datum van inwerkingtreding van deze verordening] operationeel is. Die testomgeving kan ook samen met de bevoegde autoriteiten van andere lidstaten worden opgezet. De Commissie kan technische ondersteuning, advies en instrumenten verstrekken voor de oprichting en werking van AI-testomgevingen voor regelgeving.

Aan de verplichting uit hoofde van de eerste alinea kan ook worden voldaan door deel te nemen aan een bestaande testomgeving, voor zover die deelname de deelnemende lidstaten een gelijkwaardig niveau van nationale dekking biedt.

2. Er kunnen ook aanvullende AI-testomgevingen voor regelgeving worden ontwikkeld op regionaal of lokaal niveau of samen met de bevoegde autoriteiten van andere lidstaten.
3. De Europese Toezichthouder voor gegevensbescherming kan ook een AI-testomgeving voor regelgeving opzetten voor de instellingen, organen en instanties van de Unie, en kan de rollen en taken van de nationale bevoegde autoriteiten overeenkomstig dit hoofdstuk uitoefenen.

4. De lidstaten zorgen ervoor dat de in de leden 1 en 2 bedoelde bevoegde autoriteiten voldoende middelen toewijzen om doeltreffend en tijdig aan dit artikel te voldoen. In voorkomend geval werken de nationale bevoegde autoriteiten samen met andere relevante autoriteiten en kunnen zij de betrokkenheid van andere actoren binnen het AI-ecosysteem toestaan. Dit artikel heeft geen gevolgen voor andere testomgevingen voor regelgeving die zijn ingesteld op grond van het nationale of Unierecht. De lidstaten zorgen ervoor dat de autoriteiten die toezicht houden op die andere testomgevingen en de nationale bevoegde autoriteiten voldoende met elkaar samenwerken.
5. Uit hoofde van lid 1 opgerichte AI-testomgevingen voor regelgeving voorzien in een gecontroleerde omgeving ter bevordering van innovatie en ter vergemakkelijking van het ontwikkelen, trainen, testen en valideren van innovatieve AI-systemen, volgens een specifiek, tussen de aanbieders of potentiële aanbieders en de bevoegde autoriteit overeengekomen testomgevingsplan, voor een beperkte duur voordat zij in de handel worden gebracht of in gebruik worden gesteld. Dergelijke testomgevingen kunnen inhouden dat er onder reële omstandigheden wordt getest onder toezicht binnen de testomgeving.
6. De bevoegde autoriteiten verstrekken in voorkomend geval begeleiding, toezicht en ondersteuning binnen de AI-testomgeving voor regelgeving met als doel om risico's in kaart te brengen, met name met betrekking tot de grondrechten, gezondheid en veiligheid, alsook het testen en beperkende maatregelen, en de doeltreffendheid daarvan met betrekking tot de verplichtingen en eisen van deze verordening, en, in voorkomend geval, ander Unie- en nationaal recht onder toezicht binnen de testomgeving.
7. De bevoegde autoriteiten begeleiden aanbieders en potentiële aanbieders die deelnemen aan de AI-testomgeving voor regelgeving met betrekking tot verwachtingen die voortvloeien uit de regelgeving en de wijze waarop aan de in deze verordening vastgestelde eisen en verplichtingen moet worden voldaan.

Op verzoek van de aanbieder of potentiële aanbieder van het AI-systeem verstrekt de bevoegde autoriteit een schriftelijk bewijs van de met succes in de testomgeving uitgevoerde activiteiten. De bevoegde autoriteit verstrekt ook een eindverslag waarin de in de testomgeving uitgevoerde activiteiten en de daarmee verband houdende resultaten en leerresultaten worden beschreven. Aanbieders kunnen dergelijke documentatie gebruiken om bij het conformiteitsbeoordelingsproces of relevante markttoezicht-activiteiten aan te tonen dat zij aan deze verordening voldoen. In dit verband houden markttoezichtautoriteiten en aangemelde instanties op een positieve manier rekening met de eindverslagen en de schriftelijke bewijzen die door de nationale bevoegde autoriteit worden verstrekt, teneinde de conformiteitsbeoordelingsprocedures in een redelijke mate te versnellen.

8. Met inachtneming van de vertrouwelijkheidsbepalingen van artikel 78 en met instemming van de aanbieder of potentiële aanbieder zijn de Commissie en de AI-board gemachtigd om toegang te krijgen tot de eindverslagen en houden zij er in voorkomend geval rekening mee bij de uitoefening van hun taken uit hoofde van deze verordening. Indien zowel de aanbieder of potentiële aanbieder als de nationale bevoegde autoriteit uitdrukkelijk instemmen, mag het eindverslag openbaar worden gemaakt via het in dit artikel bedoelde centrale informatieplatform.
9. Het opzetten van AI-testomgevingen voor regelgeving is erop gericht bij te dragen aan de volgende doelstellingen:
 - a) het verbeteren van de rechtszekerheid met betrekking tot het bereiken van naleving van deze verordening of, in voorkomend geval, van ander toepasselijk Unie- en nationaal recht;
 - b) ondersteunen van de uitwisseling van beste praktijken door middel van samenwerking met de autoriteiten die betrokken zijn bij de AI-testomgeving voor regelgeving;

- c) bevorderen van innovatie en concurrentievermogen en faciliteren van de ontwikkeling van een AI-ecosysteem;
 - d) bijdragen aan empirisch onderbouwd leren op het gebied van regelgeving;
 - e) vergemakkelijken en versnellen van de toegang tot de markt van de Unie voor AI-systemen, met name wanneer ze worden aangeboden door kmo's, met inbegrip van start-ups.
10. De nationale bevoegde autoriteiten zorgen ervoor dat voor zover de innovatieve AI-systemen betrekking hebben op de verwerking van persoonsgegevens of anderszins onder het toezicht van andere nationale autoriteiten of bevoegde autoriteiten vallen die toegang tot gegevens verstrekken of ondersteunen, de nationale gegevensbeschermingsautoriteiten en die andere nationale of bevoegde autoriteiten betrokken zijn bij de werking van de AI-testomgeving voor regelgeving en bij het toezicht op de aspecten die onder hun respectieve taken en bevoegdheden vallen.
11. De AI-testomgevingen voor regelgeving laten de toezichthoudende of corrigerende bevoegdheden van de bevoegde autoriteiten die toezicht houden binnen de testomgevingen onverlet, ook op regionaal of lokaal niveau. Significante risico's voor de gezondheid en veiligheid en de grondrechten die tijdens het ontwikkelen en testen van dergelijke AI-systemen worden vastgesteld, worden op adequate wijze beperkt. De nationale bevoegde autoriteiten hebben de bevoegdheid om het testproces of de deelname aan de testomgeving tijdelijk of permanent op te schorten indien doeltreffende beperkende maatregelen niet mogelijk zijn, en zij stellen het AI-bureau van een dergelijk besluit in kennis. De nationale bevoegde autoriteiten oefenen hun toezichtsbevoegdheden binnen de grenzen van het toepasselijk recht uit, waarbij zij gebruikmaken van hun discretionaire bevoegdheden bij de uitvoering van wettelijke bepalingen met betrekking tot een specifiek project inzake een AI-testomgeving voor regelgeving, met als doel innovatie op het gebied van AI in de Unie te ondersteunen.

12. Aanbieders en potentiële aanbieders die deelnemen aan de AI-testomgeving voor regelgeving blijven aansprakelijk uit hoofde van het toepasselijke Unie- en nationale aansprakelijkheidsrecht voor aan derden toegebrachte schade als gevolg van de experimenten in de testomgeving. Als de potentiële aanbieders echter het specifieke plan alsmede de voorwaarden voor hun deelname eerbiedigen en zich te goeder trouw houden aan de richtsnoeren van de nationale bevoegde autoriteit, leggen de autoriteiten geen administratieve boetes op voor de schending van deze verordening. Wanneer andere bevoegde autoriteiten die verantwoordelijk zijn voor ander Unierecht en nationaal recht actief betrokken waren bij het toezicht op het AI-systeem in de testomgeving en richtsnoeren voor naleving hebben verstrekt, worden met betrekking tot dat recht geen administratieve geldboetes opgelegd.
13. De AI-testomgevingen voor regelgeving worden zodanig ontworpen en uitgevoerd dat zij desgevallend de grensoverschrijdende samenwerking tussen nationale bevoegde autoriteiten vergemakkelijken.
14. De nationale bevoegde autoriteiten coördineren hun activiteiten en werken samen binnen het kader van de AI-board.
15. De nationale bevoegde autoriteiten stellen het AI-bureau en de AI-board in kennis van de oprichting van een testomgeving en kunnen hen om ondersteuning en begeleiding verzoeken. Er wordt door het AI-bureau een lijst van geplande en bestaande testomgevingen openbaar gemaakt en up-to-date gehouden om meer interactie in de AI-testomgevingen voor regelgeving en grensoverschrijdende samenwerking aan te moedigen.

16. De nationale bevoegde autoriteiten dienen vanaf één jaar na de oprichting van de AI-testomgeving voor regelgeving en vervolgens elk jaar tot de beëindiging ervan, bij het AI-bureau en de AI-board jaarverslagen in, alsook een afsluitend verslag. In deze verslagen wordt informatie verstrekt over de vooruitgang en de resultaten met betrekking tot de uitvoering van die testomgevingen, met inbegrip van goede praktijken, incidenten, geleerde lessen en aanbevelingen over de opzet ervan en, waar relevant, over de toepassing en mogelijke herziening van deze verordening, met inbegrip van de gedelegeerde en uitvoeringshandelingen daarvan, en over de toepassing van andere regelgeving van de Unie onder toezicht van de bevoegde autoriteiten binnen de testomgeving. De nationale bevoegde autoriteiten stellen die jaarverslagen of de samenvattingen daarvan online beschikbaar voor het publiek. De Commissie houdt in voorkomend geval rekening met de jaarverslagen bij de uitoefening van haar taken uit hoofde van deze verordening.
17. De Commissie ontwikkelt één specifieke interface met alle relevante informatie over AI-testomgevingen voor regelgeving waar belanghebbenden kunnen te communiceren met de AI-testomgevingen voor regelgeving, vragen kunnen stellen aan de bevoegde autoriteiten en niet-bindend advies kunnen krijgen over de conformiteit van innovatieve producten, diensten of bedrijfsmodellen waarin AI-technologieën zijn verwerkt, in overeenstemming met artikel 62, lid 1, punt c). De Commissie draagt in voorkomend geval zorg voor proactieve coördinatie met de nationale bevoegde autoriteiten.

Artikel 58

Gedetailleerde regelingen voor, en werking van, AI-testomgevingen voor regelgeving

1. Om versnippering in de Unie te voorkomen, stelt de Commissie uitvoeringshandelingen vast waarin de gedetailleerde regelingen worden gespecificeerd voor de instelling, de ontwikkeling, de uitvoering en de werking van AI-testomgevingen voor regelgeving en voor het toezicht erop. De uitvoeringshandelingen bevatten gemeenschappelijke beginselen met betrekking tot de volgende punten:
 - a) toelatings- en selectiecriteria voor deelname aan de AI-testomgeving voor regelgeving;
 - b) procedures voor de toepassing, deelname, monitoring, uittreding uit en beëindiging van de AI-testomgeving voor regelgeving, met inbegrip van het testomgevingsplan en het eindverslag;
 - c) de voor de deelnemers geldende voorwaarden.

Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

2. De in lid 1 bedoelde uitvoeringshandelingen waarborgen dat:
 - a) AI-testomgevingen voor regelgeving open staan voor elke aanbieder of potentiële aanbieder van een AI-systeem die voldoet aan de toelatings- en selectiecriteria, die transparant en eerlijk moeten zijn, en dat de nationale bevoegde autoriteiten aanvragers binnen drie maanden na de aanvraag in kennis stellen van hun besluit;

- b) AI-testomgevingen voor regelgeving brede en gelijke toegang bieden en de vraag om toestemming voor deelname aankunnen; aanbieders en potentiële aanbieders ook aanvragen kunnen indienen in samenwerking met gebruiksverantwoordelijken en andere relevante derden;
- c) de gedetailleerde regelingen en voorwaarden voor AI-testomgevingen voor regelgeving zo veel mogelijk flexibiliteit bieden voor nationale bevoegde autoriteiten om hun AI-testomgevingen voor regelgeving op te richten en te exploiteren;
- d) de toegang tot de AI-testomgevingen voor regelgeving voor kmo's, waaronder start-ups, kosteloos is, onverminderd uitzonderlijke kosten die de nationale bevoegde autoriteiten op billijke en evenredige wijze mogen verhalen;
- e) zij het voor aanbieders en potentiële aanbieders, door middel van de leerresultaten van de AI-testomgevingen voor regelgeving, vergemakkelijken om de conformiteitsbeoordelingsverplichtingen uit hoofde van deze verordening na te komen en de in artikel 95 bedoelde gedragscodes vrijwillig toe te passen;
- f) AI-testomgevingen voor regelgeving de betrokkenheid vergemakkelijken van andere relevante actoren binnen het AI-ecosysteem, zoals aangemelde instanties en normalisatieorganisaties, kmo's, met inbegrip van start-ups, ondernemingen, innovatoren, test- en experimenteerfaciliteiten, onderzoeks- en testlaboratoria en Europese digitale-innovatiehubs, kenniscentra en individuele onderzoekers, teneinde samenwerking met de publieke en particuliere sectoren mogelijk te maken en te vergemakkelijken;

- g) de procedures, processen en administratieve eisen voor de aanvraag, de selectie, de deelname en het vertrek uit de AI-testomgeving voor regelgeving eenvoudig en gemakkelijk te begrijpen zijn en duidelijk worden gecommuniceerd, om de deelname van kmo's, waaronder start-ups, met beperkte juridische en administratieve capaciteiten te vergemakkelijken, en in de hele Unie worden gestroomlijnd, om versnippering te voorkomen, en dat de deelname aan een door een lidstaat of de Europese Toezichthouder voor gegevensbescherming opgerichte AI-testomgeving voor regelgeving wederzijds en uniform wordt erkend en in de hele Unie dezelfde rechtsgevolgen heeft;
 - h) de deelname aan de AI-testomgeving voor regelgeving beperkt wordt tot een termijn die passend is gezien de complexiteit en de omvang van het project, en die door de nationale bevoegde autoriteit kan worden verlengd;
 - i) AI-testomgevingen voor regelgeving de ontwikkeling bevorderen van instrumenten en infrastructuur voor het testen, benchmarken, beoordelen en verklaren van de voor leren op regelgevingsgebied relevante aspecten van AI-systemen, zoals nauwkeurigheid, robuustheid en cyberbeveiliging, alsook minimalisering van de risico's voor de grondrechten, het milieu en de maatschappij in het algemeen.
3. Potentiële aanbieders in de AI-testomgevingen voor regelgeving, met name kmo's en start-ups, worden, indien van toepassing, gewezen op diensten die aan het inzetten voorafgaan, zoals begeleiding bij de uitvoering van deze verordening, op andere diensten die waarde toevoegen, zoals hulp bij normalisatiedocumenten en certificering, test- en experimenteervoorzieningen, Europese digitale-innovatiehubs en kenniscentra.

4. Indien nationale bevoegde autoriteiten overwegen toestemming te geven voor het testen onder reële omstandigheden, onder toezicht in het kader van een op grond van dit artikel op te richten AI-testomgeving voor regelgeving, komen zij specifiek met de deelnemers de voorwaarden voor die tests overeen, en met name de passende waarborgen ter bescherming van de grondrechten, de gezondheid en de veiligheid. In voorkomend geval werken zij samen met andere nationale bevoegde autoriteiten om de praktijken in de hele Unie consistent te houden.

Artikel 59

Verdere verwerking van persoonsgegevens voor het ontwikkelen van bepaalde AI-systemen in het algemeen belang in de AI-testomgeving voor regelgeving

1. In de AI-testomgeving voor regelgeving mogen rechtmatig voor andere doeleinden verzamelde persoonsgegevens uitsluitend worden verwerkt ten behoeve van het ontwikkelen, trainen en testen van bepaalde AI-systemen in de testomgeving indien aan alle volgende voorwaarden is voldaan:
- a) Er worden AI-systemen ontwikkeld zodat een overheidsinstantie of een andere natuurlijke of rechtspersoon een aanzienlijk openbaar belang kan waarborgen op een of meer van de volgende gebieden:
 - i) openbare veiligheid en volksgezondheid, met inbegrip van opsporing, diagnosticering, preventie, bestrijding en behandeling van ziekten en verbetering van gezondheidszorgstelsels;
 - ii) een hoog niveau van bescherming en verbetering van de kwaliteit van het milieu, bescherming van de biodiversiteit, bescherming tegen vervuiling, maatregelen voor de groene transitie en maatregelen ter beperking van en aanpassing aan klimaatverandering;

- iii) energieduurzaamheid;
 - iv) de veiligheid en veerkracht van vervoerssystemen en mobiliteit, kritieke vervoersinfrastructuur en vervoersnetwerken;
 - v) doeltreffendheid en kwaliteit van het openbaar bestuur en de openbare diensten;
- b) de verwerkte data zijn nodig om te voldoen aan een of meer van de in hoofdstuk III, afdeling 2, bedoelde eisen wanneer die eisen niet doeltreffend kunnen worden vervuld door het verwerken van geanonimiseerde, synthetische of andere niet persoonsgebonden data;
 - c) er zijn doeltreffende monitoringmechanismen om vast te stellen of zich tijdens de experimenten in de testomgeving hoge risico's voor de rechten en vrijheden van de betrokkenen als bedoeld in artikel 35 van Verordening (EU) 2016/679 en in artikel 39 van Verordening (EU) 2018/1725 kunnen voordoen evenals responsmechanismen om die risico's onmiddellijk te beperken en indien nodig de verwerking stop te zetten;
 - d) in het kader van de testomgeving te verwerken persoonsgegevens bevinden zich in een functioneel gescheiden, geïsoleerde en beschermde omgeving voor dataverwerking onder de controle van de potentiële aanbieder, waarbij alleen bevoegde personen toegang hebben tot deze data;
 - e) aanbieders kunnen de oorspronkelijk verzamelde gegevens alleen verder delen in overeenstemming met het Unierecht inzake gegevensbescherming; persoonsgegevens die in de testomgeving worden aangemaakt mogen niet buiten de testomgeving worden gedeeld;

- f) de verwerking van persoonsgegevens in het kader van de testomgeving mag niet leiden tot maatregelen of besluiten die gevolgen hebben voor de betrokkenen, noch gevolgen hebben voor de toepassing van hun rechten die zijn vastgelegd in het Unierecht inzake de bescherming van persoonsgegevens;
- g) in het kader van de testomgeving verwerkte persoonsgegevens worden beschermd met passende technische en organisatorische maatregelen en worden gewist nadat de deelname aan de testomgeving is beëindigd of de periode van bewaring van de persoonsgegevens ten einde is gekomen;
- h) de logbestanden van de verwerking van persoonsgegevens in het kader van de testomgeving worden bijgehouden voor de duur van de deelname aan de testomgeving, tenzij anders is bepaald in het Unierecht of het nationale recht;
- i) een volledige en gedetailleerde beschrijving van het proces en de onderbouwing van het trainen, testen en valideren van het AI-systeem wordt samen met de testresultaten bewaard als onderdeel van de in bijlage IV bedoelde technische documentatie;
- j) een korte samenvatting van het in de testomgeving ontwikkelde AI-project en de doelstellingen en verwachte resultaten ervan worden op de website van de bevoegde autoriteiten gepubliceerd; deze verplichting heeft geen betrekking op gevoelige operationele gegevens in verband met de activiteiten van rechtshandavingsinstanties en grenstoezichts-, immigratie- of asielautoriteiten.

2. Met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen voor de openbare veiligheid, onder de controle en de verantwoordelijkheid van rechtshandavingsinstanties, is de verwerking van persoonsgegevens in AI-testomgevingen voor regelgeving gebaseerd op specifiek Unie- of nationaal recht en onderworpen aan dezelfde cumulatieve voorwaarden als bedoeld in lid 1.
3. Lid 1 doet geen afbreuk aan het Unie- of nationale recht waarin verwerking voor andere doeleinden dan die uitdrukkelijk vermeld in die wetgeving wordt uitgesloten, noch aan het Unie- of nationale recht tot vaststelling van de grondslag voor de verwerking van persoonsgegevens die noodzakelijk is voor het ontwikkelen, testen of trainen van innovatieve AI-systemen of een andere rechtsgrondslag, met naleving van het Unierecht inzake de bescherming van persoonsgegevens.

Artikel 60

Testen van AI-systemen met een hoog risico onder reële omstandigheden buiten AI-testomgevingen voor regelgeving

1. AI-systemen met een hoog risico kunnen onder reële omstandigheden buiten AI-testomgevingen voor regelgeving worden getest door aanbieders of potentiële aanbieders van in bijlage III vermelde AI-systemen met een hoog risico in overeenstemming met dit artikel en het in dit artikel bedoelde plan voor tests onder reële omstandigheden, onverminderd de verbodsbepalingen krachtens artikel 5.

De Commissie specificeert, door middel van uitvoeringshandelingen, de precieze onderdelen van het plan voor tests onder reële omstandigheden. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

Dit lid doet geen afbreuk aan Unie- of nationale wetgeving voor het testen onder reële omstandigheden van AI-systemen met een hoog risico die verband houden met producten die onder de in bijlage I vermelde harmonisatiewetgeving van de Unie vallen.

2. Aanbieders of potentiële aanbieders kunnen zelf of in samenwerking met een of meer gebruiksverantwoordelijken of potentiële gebruiksverantwoordelijken onder reële omstandigheden tests uitvoeren op in bijlage III bedoelde AI-systemen met een hoog risico op elk moment vóór het in de handel brengen of in gebruik nemen van het AI-systeem.
3. Het testen van AI-systemen met een hoog risico onder reële omstandigheden uit hoofde van dit artikel doet geen afbreuk aan de ethische toetsing die op grond van het Unie- of nationale recht is vereist.
4. Aanbieders of potentiële aanbieders mogen alleen testen onder reële omstandigheden als is voldaan aan alle volgende voorwaarden:
 - a) de aanbieder of potentiële aanbieder heeft een plan voor tests onder reële omstandigheden opgesteld en ingediend bij de markttoezichtautoriteit in de lidstaat waar onder reële omstandigheden moet worden getest;
 - b) de markttoezichtautoriteit in de lidstaat waar onder reële omstandigheden moet worden getest, heeft het testen onder reële omstandigheden en het plan voor tests onder reële omstandigheden goedgekeurd; indien de markttoezichtautoriteit binnen 30 dagen geen antwoord heeft gegeven, worden het testen onder reële omstandigheden en het plan voor tests onder reële omstandigheden geacht te zijn goedgekeurd; indien het nationale recht niet voorziet in een stilzwijgende goedkeuring, blijft het testen onder reële omstandigheden onderworpen aan een toestemming;

- c) de aanbieder of potentiële aanbieder, met uitzondering van aanbieders of potentiële aanbieders van in de punten 1, 6 en 7 van bijlage III bedoelde AI-systemen met een hoog risico op de gebieden rechtshandhaving, migratie, asiel en grenstoezichtsbeheer en AI-systemen met een hoog risico als bedoeld in punt 2 van bijlage III, heeft het testen onder reële omstandigheden geregistreerd overeenkomstig artikel 71, lid 4, met een Uniebreed uniek identificatienummer en de in bijlage IX gespecificeerde informatie; de aanbieder of potentiële aanbieder van in de punten 1, 6 en 7 van bijlage III bedoelde AI-systemen met een hoog risico op de gebieden van rechtshandhaving, migratie, asiel en grenstoezichtsbeheer, heeft het testen onder reële omstandigheden geregistreerd in het beveiligde niet-openbare gedeelte van de EU-databank overeenkomstig artikel 49, lid 4, punt d), met een Uniebreed uniek identificatienummer en de daarin gespecificeerde informatie; de aanbieder of potentiële aanbieder van in punt 2 van bijlage III bedoelde AI-systemen met een hoog risico heeft het testen onder reële omstandigheden geregistreerd overeenkomstig artikel 49, lid 5.
- d) de aanbieder of potentiële aanbieder die onder reële omstandigheden test, is in de Unie gevestigd of heeft een in de Unie gevestigde wettelijke vertegenwoordiger aangewezen;
- e) gegevens die zijn verzameld en verwerkt met het oog op het testen onder reële omstandigheden mogen alleen aan derde landen worden doorgegeven mits er passende en toepasselijke waarborgen uit hoofde van het Unierecht worden toegepast;

- f) het testen onder reële omstandigheden duurt niet langer dan nodig is om de doelstellingen ervan te verwezenlijken en in geen geval langer dan zes maanden, met een mogelijke verlenging van nog eens zes maanden indien de aanbieder of potentiële aanbieder de markttoezichtautoriteit daar vooraf van in kennis stelt, met een uitleg waarom een dergelijke verlenging noodzakelijk is;
- g) proefpersonen die onder reële omstandigheden worden getest en die tot kwetsbare groepen behoren vanwege hun leeftijd of handicap, worden naar behoren beschermd;
- h) indien een aanbieder of potentiële aanbieder het testen onder reële omstandigheden organiseert in samenwerking met een of meer gebruiksverantwoordelijken of potentiële gebruiksverantwoordelijken, worden zij geïnformeerd over alle aspecten van het testen die relevant zijn voor hun beslissing om deel te nemen, en krijgen zij de relevante gebruiksinstructies van het AI-systeem als bedoeld in artikel 13; de aanbieder of potentiële aanbieder en de gebruiksverantwoordelijke of potentiële gebruiksverantwoordelijke sluiten een overeenkomst waarin hun taken en verantwoordelijkheden worden gespecificeerd teneinde te waarborgen dat de bepalingen voor het testen onder reële omstandigheden uit hoofde van deze verordening en ander toepasselijk Unie- en nationaal recht worden nageleefd;
- i) de proefpersonen die onder reële omstandigheden worden getest, hebben geïnformeerde toestemming gegeven overeenkomstig artikel 61, of, in het geval van rechtshandhaving, indien het vragen om geïnformeerde toestemming het testen van het AI-systeem onder reële omstandigheden onmogelijk zou maken, de test zelf en het resultaat van de test onder reële omstandigheden hebben geen negatieve gevolgen voor de proefpersonen en hun persoonsgegevens worden na de uitvoering van test gewist;

- j) op het testen onder reële omstandigheden wordt daadwerkelijk toezicht gehouden door de aanbieder of potentiële aanbieder, alsook door gebruiksverantwoordelijken of potentiële gebruiksverantwoordelijken via personen die voldoende zijn gekwalificeerd op het relevante gebied en beschikken over de nodige capaciteiten, opleiding en bevoegdheden om hun taken uit te voeren;
- k) de voorspellingen, aanbevelingen of beslissingen van het AI-systeem kunnen daadwerkelijk worden teruggedraaid en genegeerd.

- 5. Proefpersonen van het testen onder reële omstandigheden of hun wettelijke vertegenwoordiger, al naargelang het geval, kunnen zich, zonder nadelige gevolgen en zonder enige rechtvaardiging, te allen tijde uit het testen terugtrekken door hun geïnformeerde toestemming in te trekken, waarna zij om de onmiddellijke en permanente verwijdering van hun persoonsgegevens kunnen verzoeken. De intrekking van de geïnformeerde toestemming heeft geen gevolgen voor de reeds uitgevoerde activiteiten.
- 6. Overeenkomstig artikel 75 verlenen de lidstaten hun markttoezichtautoriteiten de bevoegdheid om aanbieders en potentiële aanbieders te verplichten informatie te verstrekken, om onaangekondigde inspecties op afstand of ter plaatse uit te voeren en om toezicht te houden op de uitvoering van het testen onder reële omstandigheden en de aanverwante AI-systemen met een hoog risico. Markttoezichtautoriteiten gebruiken deze bevoegdheden om ervoor te zorgen dat het testen onder reële omstandigheden zich veilig kan ontwikkelen.

7. Elk ernstig incident dat tijdens het testen onder reële omstandigheden wordt vastgesteld, wordt gemeld bij de nationale markttoezichtautoriteit overeenkomstig artikel 73. De aanbieder of potentiële aanbieder neemt onmiddellijke risicobeperkende maatregelen of, bij gebreke daarvan, schorst het testen onder reële omstandigheden totdat dergelijke risicobeperkende maatregelen zijn getroffen, of beëindigt anders het testen. De aanbieder of potentiële aanbieder stelt een procedure vast voor het onmiddellijk terugroepen van het AI-systeem bij een dergelijke beëindiging van het testen onder reële omstandigheden.
8. Aanbieders of potentiële aanbieders stellen de nationale markttoezichtautoriteit in de lidstaat waar er onder reële omstandigheden moet worden getest, in kennis van de opschorting of beëindiging van het testen onder reële omstandigheden en van de eindresultaten.
9. De aanbieder of potentiële aanbieder zijn aansprakelijk op grond van het toepasselijke Unie- en nationale aansprakelijkheidsrecht voor schade die tijdens het testen onder reële omstandigheden wordt veroorzaakt.

Artikel 61

Geïnformeerde toestemming om deel te nemen aan

het testen onder reële omstandigheden buiten AI-testomgevingen voor regelgeving

1. Met het oog op het testen onder reële omstandigheden overeenkomstig artikel 60 moet van de proefpersonen vrijwillig gegeven geïnformeerde toestemming worden verkregen voorafgaand aan hun deelname aan het testen en nadat zij naar behoren zijn geïnformeerd en beknopte, duidelijke, relevante en begrijpelijke informatie hebben gekregen over:
 - a) de aard en de doelstellingen van het testen onder reële omstandigheden en de mogelijke ongemakken die verband kunnen houden met hun deelname;
 - b) de voorwaarden waaronder in reële omstandigheden moet worden getest, met inbegrip van de verwachte duur van de deelname van de proefpersoon of proefpersonen;
 - c) hun rechten en de garanties met betrekking tot hun deelname, met name hun recht om te weigeren deel te nemen aan, en het recht om zich te allen tijde terug te trekken uit, het testen onder reële omstandigheden zonder daarvan enig nadeel te ondervinden en zonder zich te hoeven rechtvaardigen;
 - d) de afspraken met betrekking tot het aanvragen van het terugdraaien of negeren van de voorspellingen, aanbevelingen of beslissingen van het AI-systeem;
 - e) het Uniebrede unieke identificatienummer van het testen onder reële omstandigheden overeenkomstig artikel 60, lid 4, punt c), en de contactgegevens van de aanbieder of zijn wettelijke vertegenwoordiger bij wie nadere informatie kan worden verkregen.

2. De geïnformeerde toestemming wordt gedateerd en gedocumenteerd en er wordt een kopie verstrekt aan de proefpersonen of hun wettelijke vertegenwoordiger.

Artikel 62

Maatregelen voor aanbieders en gebruiksverantwoordelijken, met name kmo's, met inbegrip van start-ups

1. De lidstaten ondernemen de volgende acties:
 - a) kmo's, met inbegrip van start-ups, die een maatschappelijke zetel of een bijkantoor in de Unie hebben, prioritaire toegang verlenen tot de AI-testomgevingen voor regelgeving voor zover zij aan de toelatingsvoorwaarden en selectiecriteria voldoen; de prioritaire toegang sluit niet uit dat andere dan de in dit lid bedoelde kmo's, met inbegrip van start-ups, toegang krijgen tot de AI-testomgeving voor regelgeving, mits zij ook aan de toelatingsvoorwaarden en selectiecriteria voldoen;
 - b) specifieke bewustmakings- en opleidingsactiviteiten organiseren over de toepassing van deze verordening, afgestemd op de behoeften van kmo's, met inbegrip van start-ups, gebruiksverantwoordelijken en, in voorkomend geval, lokale overheidsinstanties;
 - c) bestaande specifieke communicatiekanalen benutten en, waar passend, nieuwe opzetten voor communicatie met kmo's, met inbegrip van start-ups, gebruiksverantwoordelijken, andere innovatoren en, in voorkomend geval, lokale overheidsinstanties, om advies te verstrekken en te reageren op vragen over de uitvoering van deze verordening, onder meer met betrekking tot deelname aan AI-testomgevingen voor regelgeving;

- d) de deelname van kmo's en andere relevante belanghebbenden aan het proces voor de ontwikkeling van normen faciliteren.
2. De specifieke belangen en behoeften van aanbieders die kmo's zijn, met inbegrip van start-ups, worden in aanmerking genomen bij het bepalen van de vergoedingen voor conformiteitsbeoordelingen krachtens artikel 43, waarbij die vergoedingen naar evenredigheid van hun omvang, de omvang van de markt en andere relevante indicatoren worden verlaagd.
3. Het AI-bureau onderneemt de volgende acties:
- a) het verstrekken van gestandaardiseerde sjablonen voor de gebieden die onder deze verordening vallen, zoals gespecificeerd door de AI-board in zijn verzoek;
 - b) het ontwikkelen en in stand houden van een centraal informatieplatform dat gemakkelijk te gebruiken informatie met betrekking tot deze verordening biedt aan alle operatoren in de hele Unie;
 - c) het organiseren van passende voorlichtingscampagnes om meer bekendheid te geven aan de uit deze verordening voortvloeiende verplichtingen;
 - d) het evalueren en bevorderen van de convergentie van beste praktijken bij openbare aanbestedingsprocedures met betrekking tot AI-systemen.

Artikel 63

Afwijkingen voor specifieke operatoren

1. Micro-ondernemingen in de zin van Aanbeveling 2003/361/EG kunnen op vereenvoudigde wijze voldoen aan bepaalde elementen van het bij artikel 17 van deze verordening vereiste systeem voor kwaliteitsbeheer, mits zij geen partner-ondernemingen of verbonden ondernemingen in de zin van die aanbeveling hebben. Daartoe ontwikkelt de Commissie richtsnoeren over de elementen van het systeem voor kwaliteitsbeheer waaraan op vereenvoudigde wijze kan worden voldaan, rekening houdend met de behoeften van micro-ondernemingen, zonder afbreuk te doen aan het beschermingsniveau of de noodzaak om de verplichtingen voor AI-systemen met een hoog risico na te leven.
2. Lid 1 van dit artikel wordt niet zodanig geïnterpreteerd dat die operatoren worden vrijgesteld van de naleving van andere in deze verordening vastgelegde eisen of verplichtingen, met inbegrip van die welke zijn vastgelegd in de artikelen 9, 10, 11, 12, 13, 14, 15, 72 en 73.

Hoofdstuk VII

Governance

AFDELING 1

GOVERNANCE OP UNIENIVEAU

Artikel 64

AI-bureau

1. De Commissie ontwikkelt deskundigheid en capaciteiten op Unieniveau op het gebied van AI via het AI-bureau.
2. De lidstaten faciliteren de aan het AI-bureau toevertrouwde taken, zoals weergegeven in deze verordening.

Artikel 65

Oprichting en structuur van de Europese raad voor artificiële intelligentie

1. Hierbij wordt een Europese raad voor artificiële intelligentie (European Artificial Intelligence Board - de “AI-board”) opgericht.

2. De AI-board bestaat uit één vertegenwoordiger per lidstaat. De Europese Toezichthouder voor gegevensbescherming neemt deel als waarnemer. Het AI-bureau woont ook de vergaderingen van de AI-board bij zonder aan de stemmingen deel te nemen. De AI-board kan per geval andere autoriteiten, organen of deskundigen van de lidstaten en de Unie voor de vergaderingen uitnodigen, indien de besproken zaken voor hen van belang zijn.
3. Elke vertegenwoordiger wordt door zijn lidstaat aangewezen voor een periode van drie jaar, die eenmaal kan worden verlengd.
4. De lidstaten zorgen ervoor dat hun vertegenwoordigers in de AI-board:
- a) in hun lidstaat over de toepasselijke bevoegdheden beschikken om actief bij te dragen tot de vervulling van de in artikel 66 genoemde taken van de AI-board;
 - b) worden aangewezen als één contactpunt voor de AI-board en, in voorkomend geval, rekening houdend met de behoeften van de lidstaten, als één contactpunt voor belanghebbenden;
 - c) bevoegd zijn om de samenhang en coördinatie tussen de nationale bevoegde autoriteiten in hun lidstaat met betrekking tot de uitvoering van deze verordening te vergemakkelijken, onder meer door het verzamelen van relevante gegevens en informatie met het oog op de vervulling van hun taken in de AI-board.
5. De aangewezen vertegenwoordigers van de lidstaten stellen het reglement van orde van de AI-board met een tweederdemeerderheid vast. In het reglement van orde worden met name procedures vastgelegd voor de selectieprocedure, de duur van het mandaat van en de specificaties van de taken van de voorzitter, gedetailleerde stemprocedures en de organisatie van de activiteiten van de AI-board en van zijn subgroepen.

6. De AI-board richt twee permanente subgroepen op om een platform te bieden voor samenwerking en uitwisseling tussen markttoezichtautoriteiten en aanmeldende autoriteiten over kwesties betreffende respectievelijk markttoezicht en aangemelde instanties.

De permanente subgroep voor markttoezicht moet fungeren als de administratieve-samenwerkingsgroep (ADCO) voor deze verordening in de zin van artikel 30 van Verordening (EU) 2019/1020.

De AI-board kan in voorkomend geval andere permanente of tijdelijke subgroepen oprichten om specifieke kwesties te onderzoeken. In voorkomend geval kunnen vertegenwoordigers van het in artikel 67 bedoelde adviesforum als waarnemer worden uitgenodigd voor dergelijke subgroepen of voor specifieke vergaderingen van die subgroepen.

7. De AI-board is zodanig georganiseerd en functioneert zodanig dat de objectiviteit en onpartijdigheid van zijn activiteiten gewaarborgd zijn.

8. De AI-board wordt voorgezeten door een van de vertegenwoordigers van de lidstaten. Het AI-bureau verzorgt het secretariaat van de AI-board, roept op verzoek van de voorzitter de vergaderingen bijeen en stelt de agenda op overeenkomstig de taken van de AI-board krachtens deze verordening en overeenkomstig zijn reglement.

Artikel 66

Taken van de AI-board

De AI-board adviseert en assisteert de Commissie en de lidstaten teneinde de consistente en doeltreffende toepassing van deze verordening te vergemakkelijken. Daartoe kan de AI-board met name:

- a) bijdragen aan de coördinatie tussen de nationale bevoegde autoriteiten die verantwoordelijk zijn voor de toepassing van deze verordening en, in samenwerking met en met instemming van de betrokken markttoezichtautoriteiten, de in artikel 74, lid 11, bedoelde gezamenlijke activiteiten van de markttoezichtautoriteiten ondersteunen;
- b) technische en regelgevingsexpertise en beste praktijken onder de lidstaten verzamelen en delen;
- c) advies verstrekken over de uitvoering van deze verordening, met name wat betreft de handhaving van de regels inzake AI-modellen voor algemene doeleinden;
- d) bijdragen tot de harmonisatie van de administratieve praktijken in de lidstaten, onder meer met betrekking tot de in artikel 46 bedoelde afwijking van de conformiteits-beoordelingsprocedures, de werking van AI-testomgevingen voor regelgeving en het testen onder reële omstandigheden als bedoeld in de artikelen 57, 59 en 60;

- e) op verzoek van de Commissie of op eigen initiatief aanbevelingen en schriftelijke adviezen uitbrengen over alle relevante aangelegenheden in verband met de uitvoering van deze verordening en de consistente en doeltreffende toepassing ervan, waaronder:
- i) over de ontwikkeling en toepassing van praktijkcodes en praktijkcodes op grond van deze verordening, alsmede van de richtsnoeren van de Commissie;
 - ii) over de evaluatie en toetsing van deze verordening op grond van artikel 112, onder meer met betrekking tot de in artikel 73 bedoelde meldingen van ernstige incidenten en de werking van de in artikel 71 bedoelde EU-databank, de voorbereiding van de gedelegeerde of uitvoeringshandelingen, en met betrekking tot mogelijke afstemming van deze verordening op de in bijlage I vermelde harmonisatiewetgeving van de Unie;
 - iii) over technische specificaties of bestaande normen ten aanzien van de in hoofdstuk III, afdeling 2, beschreven eisen;
 - iv) over het gebruik van geharmoniseerde normen of gemeenschappelijke specificaties als bedoeld in de artikelen 40 en 41;
 - v) over trends, bijvoorbeeld met betrekking tot het Europese mondiale concurrentievermogen op het gebied van AI, de invoering van AI in de Unie en de ontwikkeling van digitale vaardigheden;
 - vi) over trends met betrekking tot de steeds veranderende typologie van AI-waardeketens, met name wat de daaruit voortvloeiende gevolgen voor de verantwoordingsplicht betreft;

- vii) over de eventuele noodzaak van een wijziging van bijlage III overeenkomstig artikel 7, en over de eventuele noodzaak van een mogelijke herziening van artikel 5 op grond van artikel 112, rekening houdend met de op dat gebied beschikbare gegevens en de meest recente technologische ontwikkelingen;
- f) de Commissie ondersteunen bij het promoten van AI-geletterdheid en het brede publiek beter bekendmaken met en meer inzicht verschaffen in de voordelen, de risico's, de waarborgen en de rechten en plichten in verband met het gebruik van AI-systemen;
- g) de ontwikkeling bevorderen van gemeenschappelijke criteria en een gedeeld begrip tussen marktdeelnemers en bevoegde autoriteiten met betrekking tot de relevante concepten waarin deze verordening voorziet, onder meer door bij te dragen aan de ontwikkeling van benchmarks;
- h) waar passend samenwerken met andere instellingen, organen en instanties van de Unie, alsook relevante deskundigengroepen en -netwerken van de Unie, met name op het gebied van productveiligheid, cyberbeveiliging, mededinging, digitale en mediadiensten, financiële diensten, consumentenbescherming, gegevensbescherming en bescherming van de grondrechten;
- i) bijdragen aan doeltreffende samenwerking met de bevoegde autoriteiten van derde landen en met internationale organisaties;
- j) de nationale bevoegde autoriteiten en de Commissie bijstaan bij de ontwikkeling van de organisatorische en technische deskundigheid die nodig zijn voor de uitvoering van deze verordening, onder meer door bij te dragen aan de beoordeling van de opleidingsbehoeften voor personeel van de lidstaten dat betrokken is bij de uitvoering van deze verordening;

- k) het AI-bureau bijstaan bij het ondersteunen van nationale bevoegde autoriteiten bij het opzetten en ontwikkelen van AI-testomgevingen voor regelgeving, en samenwerking en informatie-uitwisseling tussen AI-testomgevingen voor regelgeving vergemakkelijken;
- l) bijdragen aan of relevant advies verstrekken over de ontwikkeling van richtsnoeren;
- m) de Commissie adviseren over internationale aangelegenheden op het gebied van AI;
- n) adviezen verstrekken aan de Commissie over de gekwalificeerde waarschuwingen met betrekking tot AI-modellen voor algemene doeleinden;
- o) adviezen van de lidstaten ontvangen over gekwalificeerde waarschuwingen met betrekking tot AI-modellen voor algemene doeleinden, en over nationale ervaringen en praktijken met betrekking tot de monitoring en handhaving van AI-systemen, met name systemen waarin de AI-modellen voor algemene doeleinden zijn geïntegreerd.

Artikel 67

Adviesforum

1. Er wordt een adviesforum opgericht om technische expertise te verstrekken en de AI-board en de Commissie te adviseren, alsook bij te dragen aan hun taken uit hoofde van deze verordening.
2. De samenstelling van het adviesforum vertegenwoordigt een evenwichtige selectie van belanghebbenden, waaronder het bedrijfsleven, start-ups, kmo's, het maatschappelijk middenveld en de academische wereld. Bij de samenstelling van het adviesforum wordt een evenwicht in acht genomen tussen commerciële en niet-commerciële belangen en, binnen de categorie commerciële belangen, tussen kmo's en andere ondernemingen.

3. De Commissie benoemt de leden van het adviesforum, overeenkomstig de criteria van lid 2, uit belanghebbenden met erkende deskundigheid op het gebied van AI.
4. De ambtstermijn van de leden van het adviesforum bedraagt twee jaar en kan met ten hoogste vier jaar worden verlengd.
5. Het Bureau voor de grondrechten, Enisa, het Europees Comité voor Normalisatie (CEN), het Europees Comité voor elektrotechnische normalisatie (CENELEC) en het Europees Instituut voor telecommunicatienormen (ETSI) zijn permanente leden van het adviesforum.
6. Het adviesforum stelt zijn reglement vast. Het kiest uit zijn leden twee covoorzitters, op basis van de criteria van lid 2. De ambtstermijn van de covoorzitters bedraagt twee jaar en kan één keer worden verlengd.
7. Het adviesforum belegt minstens twee keer per jaar een vergadering. Het adviesforum kan deskundigen en andere belanghebbenden uitnodigen om zijn vergaderingen bij te wonen.
8. Het adviesforum kan op verzoek van de AI-board of de Commissie adviezen, aanbevelingen en schriftelijke bijdragen opstellen.
9. Het adviesforum kan in voorkomend geval permanente of tijdelijke subgroepen oprichten om specifieke vraagstukken met betrekking tot de doelstellingen van deze verordening te onderzoeken.
10. Het adviesforum stelt een jaarverslag over zijn activiteiten op. Dat verslag wordt openbaar gemaakt.

Artikel 68

Wetenschappelijk panel van onafhankelijke deskundigen

1. De Commissie stelt door middel van een uitvoeringshandeling bepalingen vast betreffende de oprichting van een wetenschappelijk panel van onafhankelijke deskundigen (het “wetenschappelijke panel”) ter ondersteuning van de handhavingsactiviteiten in het kader van deze verordening. Die uitvoeringshandeling wordt vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.
2. Het wetenschappelijk panel bestaat uit deskundigen die door de Commissie zijn geselecteerd op basis van de actuele wetenschappelijke of technische deskundigheid op het gebied van AI die nodig is voor de in lid 3 bedoelde taken. Het wetenschappelijk panel kan aantonen dat het voldoet aan alle volgende voorwaarden:
 - a) beschikken over bijzondere deskundigheid en competenties en wetenschappelijke of technische deskundigheid op het gebied van AI;
 - b) onafhankelijkheid van aanbieders van AI-systemen of AI-modellen voor algemene doeleinden;
 - c) het vermogen om activiteiten zorgvuldig, nauwkeurig en objectief uit te voeren.

De Commissie bepaalt in overleg met de AI-board het aantal deskundigen in het panel in overeenstemming met de vereiste behoeften en zorgt voor een eerlijke gender- en geografische vertegenwoordiging.

3. Het wetenschappelijk panel adviseert en ondersteunt het AI-bureau, met name op het gebied van de volgende taken:
- a) het ondersteunen van de uitvoering en handhaving van deze verordening met betrekking tot AI-modellen en -systemen voor algemene doeleinden, met name door:
 - i) het AI-bureau te waarschuwen voor mogelijke systeemrisico's op Unieniveau van AI-modellen voor algemene doeleinden, overeenkomstig artikel 90;
 - ii) bij te dragen aan de ontwikkeling van instrumenten en methoden voor de evaluatie van de capaciteiten van AI-modellen en -systemen voor algemene doeleinden, onder meer door middel van benchmarks;
 - iii) advies te verstrekken over de classificatie van AI-modellen voor algemene doeleinden met een systeemrisico;
 - iv) advies te verstrekken over de classificatie van verschillende AI-modellen en -systemen voor algemene doeleinden;
 - v) bij te dragen aan de ontwikkeling van instrumenten en sjablonen;
 - b) het ondersteunen van de werkzaamheden van markttoezichtautoriteiten op hun verzoek;
 - c) het ondersteunen van in artikel 74, lid 11, bedoelde grensoverschrijdende markttoezichtactiviteiten, onverminderd de bevoegdheden van de markttoezichtautoriteiten;

- d) het ondersteunen van het AI-bureau bij de uitvoering van haar taken in het kader van de vrijwaringsprocedure van de Unie uit hoofde van artikel 81.
4. De deskundigen in het wetenschappelijk panel voeren hun taken onpartijdig en objectief uit en waarborgen de vertrouwelijkheid van de informatie en gegevens die zij bij de uitvoering van hun taken en activiteiten verkrijgen. Zij vragen noch aanvaarden instructies van wie dan ook bij de uitoefening van hun taken uit hoofde van lid 3. Elke deskundige stelt een belangenverklaring op, die openbaar wordt gemaakt. Het AI-bureau zorgt voor systemen en procedures voor het actief beheren en voorkomen van mogelijke belangenconflicten.
5. De in lid 1 bedoelde uitvoeringshandeling bevat bepalingen over de voorwaarden, procedures en gedetailleerde regelingen voor het wetenschappelijk panel en de leden daarvan om waarschuwingen af te geven en om het AI-bureau om bijstand te verzoeken voor de uitvoering van de taken van het wetenschappelijk panel.

Artikel 69

Toegang tot de pool van deskundigen door de lidstaten

1. De lidstaten kunnen een beroep doen op deskundigen van het wetenschappelijk panel ter ondersteuning van hun handhavingsactiviteiten in het kader van deze verordening.

2. De lidstaten kan worden voorgeschreven dat zij een vergoeding betalen voor het advies en de ondersteuning van de deskundigen. De structuur en de hoogte van de vergoedingen en de schaal en structuur van de invorderbare kosten worden in de in artikel 68, lid 1 bedoelde uitvoeringshandeling vermeld, rekening houdend met de doelstellingen van een adequate uitvoering van deze verordening, de kosteneffectiviteit en de noodzaak ervoor te zorgen dat alle lidstaten daadwerkelijk toegang tot de deskundigen hebben.
3. De Commissie vergemakkelijkt de tijdige toegang van de lidstaten tot de deskundigen, voor zover nodig, en zorgt ervoor dat de combinatie van ondersteunende activiteiten door Europese ondersteunende structuren voor AI-testen op grond van artikel 84 en deskundigen uit hoofde van dit artikel uitvoeren, efficiënt wordt georganiseerd en de best mogelijke toegevoegde waarde oplevert.

AFDELING 2

NATIONALE BEVOEGDE AUTORITEITEN

Artikel 70

Aanwijzing van nationale bevoegde autoriteiten en centrale contactpunten

1. Elke lidstaat moet voor de toepassing van deze verordening ten minste één aanmeldende autoriteit en ten minste één markttoezichtautoriteit instellen of aanwijzen als nationale bevoegde autoriteiten. Die nationale bevoegde autoriteiten moeten hun bevoegdheden onafhankelijk, onpartijdig en onbevooroordeeld uitoefenen, teneinde de objectiviteit van hun activiteiten en taken te waarborgen en de toepassing en uitvoering van deze verordening te verzekeren. De leden van die autoriteiten onthouden zich van handelingen die onverenigbaar zijn met hun ambt. Op voorwaarde dat deze beginselen in acht worden genomen, kunnen die activiteiten en taken door een of meer aangewezen autoriteiten worden uitgevoerd, in overeenstemming met de organisatorische behoeften van de lidstaat.
2. De lidstaten verstrekken de Commissie informatie over de identiteit en de taken van de aanmeldende autoriteiten en de markttoezichtautoriteiten, alsook over eventuele latere wijzigingen daarin. De lidstaten maken uiterlijk op ... [12 maanden na de datum van inwerkingtreding van deze verordening] via elektronische communicatiemiddelen informatie bekend over de wijze waarop met de bevoegde autoriteiten en centrale contactpunten contact kan worden opgenomen. De lidstaten wijzen een markttoezichtautoriteit aan die optreedt als centraal contactpunt voor deze verordening en stellen de Commissie in kennis van de identiteit van het centrale contactpunt. De Commissie maakt een lijst van de centrale contactpunten openbaar.

3. De lidstaten zorgen ervoor dat hun nationale bevoegde autoriteiten over voldoende technische, financiële en personele middelen en over passende infrastructuur beschikken om hun taken krachtens deze verordening op doeltreffende wijze uit te voeren. De nationale bevoegde autoriteiten beschikken met name over voldoende permanent beschikbaar personeel waarvan de competenties en expertise bestaan uit een grondig inzicht in AI-technologieën, gegevens en gegevensverwerking, bescherming van persoonsgegevens, cyberbeveiliging, grondrechten, gezondheids- en veiligheidsrisico's en kennis van bestaande normen en wettelijke eisen. De lidstaten beoordelen en, indien nodig, actualiseren de in dit lid bedoelde benodigde competenties en middelen jaarlijks.
4. De nationale bevoegde autoriteiten nemen passende maatregelen om te zorgen voor een adequaat niveau van cyberbeveiliging.
5. Bij de uitvoering van hun taken voldoen de nationale bevoegde autoriteiten aan de in artikel 78 vastgelegde vertrouwelijkheidsverplichtingen.
6. Uiterlijk op ... [één jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de twee jaar, brengen de lidstaten aan de Commissie verslag uit over de stand van zaken met betrekking tot de financiële en personele middelen van de nationale bevoegde autoriteiten, met een beoordeling van de toereikendheid ervan. De Commissie bezorgt die informatie ter bespreking en voor mogelijke aanbevelingen aan de AI-board.
7. De Commissie bevordert de uitwisseling van ervaringen tussen de nationale bevoegde autoriteiten.

8. Nationale bevoegde autoriteiten kunnen begeleiding bij en advies over de uitvoering van deze verordening verstrekken, met name aan kmo's, met inbegrip van start-ups, rekening houdend met de begeleiding en het advies van de AI-board en, indien nodig, de Commissie. Wanneer nationale bevoegde autoriteiten van plan zijn te voorzien in begeleiding en advies ten aanzien van een AI-systeem op gebieden die onder ander Unierecht vallen, worden in voorkomend geval de nationale bevoegde autoriteiten onder dat Unierecht geraadpleegd.
9. Indien instellingen, organen of instanties van de Unie binnen het toepassingsgebied van deze verordening vallen, treedt de Europese Toezichthouder voor gegevensbescherming op als de bevoegde autoriteit voor het toezicht daarop.

Hoofdstuk VIII

EU-databank voor AI-systemen met een hoog risico

Artikel 71

EU-databank voor in bijlage III vermelde AI-systemen met een hoog risico

1. De Commissie zorgt in samenwerking met de lidstaten voor het opzetten en onderhouden van een EU-databank met de in de leden 2 en 3 van dit artikel bedoelde informatie betreffende in artikel 6, lid 2, bedoelde AI-systemen met een hoog risico die overeenkomstig de artikelen 49 en 60 zijn geregistreerd en AI-systemen die niet als AI-systemen met een hoog risico worden beschouwd op grond van artikel 6, lid 3, en die zijn geregistreerd overeenkomstig artikel 6, lid 4 en artikel 49. Bij het vaststellen van de functionele specificaties van een dergelijke databank raadpleegt de Commissie de deskundigen ter zake, en bij het bijwerken van die functionele specificaties raadpleegt de Commissie de AI-board.

2. De in afdelingen A en B van bijlage VIII vermelde gegevens worden in de EU-databank ingevoerd door de aanbieder of, in voorkomend geval, de gemachtigde.
3. De in afdeling C van bijlage VIII vermelde gegevens worden in de EU-databank ingevoerd door de gebruiksverantwoordelijke die, overeenkomstig artikel 49, leden 3 en 4, een overheidsinstantie, agentschap of orgaan is of namens hen optreedt.
4. Uitgezonderd voor het in artikel 49, lid 4, en artikel 60, lid 4, punt c), bedoelde deel is de informatie in de overeenkomstig artikel 49 geregistreerde EU-databank op gebruikersvriendelijke wijze openbaar toegankelijk. De informatie moet gemakkelijk te doorzoeken en machineleesbaar zijn. De overeenkomstig artikel 60 geregistreerde informatie is alleen toegankelijk voor markttoezichtautoriteiten en de Commissie, tenzij de aanbieder of potentiële aanbieder toestemming heeft gegeven om de informatie ook toegankelijk te maken voor het publiek.
5. De EU-databank bevat alleen persoonsgegevens voor zover die nodig zijn voor het verzamelen en verwerken van informatie overeenkomstig deze verordening. Die informatie bevat de namen en contactgegevens van natuurlijke personen die verantwoordelijk zijn voor de registratie van het systeem en wettelijk gemachtigd zijn de aanbieder of de gebruiksverantwoordelijke, naargelang het geval, te vertegenwoordigen.
6. De Commissie is voor de EU-databank de verantwoordelijke voor de verwerking. Zij stelt adequate technische en administratieve ondersteuning ter beschikking van aanbieders, potentiële aanbieders en gebruiksverantwoordelijken. De EU-databank voldoet aan de toepasselijke toegankelijkheidseisen.

Hoofdstuk IX

Monitoring na het in de handel brengen, informatie-uitwisseling en markttoezicht

AFDELING 1

MONITORING NA HET IN DE HANDEL BRENGEN

Artikel 72

*Monitoring door aanbieders na het in de handel brengen en plan voor monitoring
na het in de handel brengen voor AI-systemen met een hoog risico*

1. Aanbieders moeten een systeem voor monitoring na het in de handel brengen vaststellen en documenteren op een manier die evenredig is aan de aard van de AI-technologieën en de risico's van het AI-systeem met een hoog risico.
2. Het systeem voor monitoring na het in de handel brengen verzamelt, documenteert en analyseert actief en systematisch relevante data die door gebruiksverantwoordelijken kunnen zijn verstrekt of via andere bronnen kunnen zijn verzameld, over de prestaties van AI-systemen met een hoog risico gedurende hun hele levensduur, en die de aanbieder in staat stellen na te gaan of AI-systemen blijvend voldoen aan de in hoofdstuk III, afdeling 2, vermelde voorschriften. In voorkomend geval omvat de monitoring na het in de handel brengen een analyse van de interactie met andere AI-systemen. Deze verplichting geldt niet voor gevoelige operationele gegevens van gebruiksverantwoordelijken die rechtshandhavingsinstanties zijn.

3. Het systeem voor monitoring na het in de handel brengen is gebaseerd op een plan voor monitoring na het in de handel brengen. Het plan voor monitoring na het in de handel brengen maakt deel uit van de in bijlage IV bedoelde technische documentatie. De Commissie stelt uiterlijk op ... [18 maanden na de inwerkingtreding van deze verordening] een uitvoeringshandeling vast met gedetailleerde bepalingen voor het opstellen van een model voor het plan voor monitoring na het in de handel brengen en de lijst van elementen die in het plan moeten worden opgenomen. De uitvoeringshandeling wordt volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure vastgesteld.
4. Voor AI-systemen met een hoog risico die onder de in afdeling A van bijlage I vermelde harmonisatiewetgeving van de Unie vallen, hebben aanbieders, indien er krachtens die wetgeving reeds een systeem en een plan voor monitoring na het in de handel brengen zijn vastgesteld, ten behoeve van de consistentie, ter vermijding van dubblures en om extra lasten tot een minimum te beperken, de keuze om de noodzakelijke in de leden 1, 2 en 3 beschreven elementen te integreren, met gebruikmaking van het in lid 3 bedoelde model, in systemen en plannen die reeds bestaan op grond van die wetgeving, mits dat een gelijkwaardig beschermingsniveau garandeert.

De eerste alinea van dit lid is ook van toepassing op in punt 5 van bijlage III bedoelde AI-systemen met een hoog risico die in de handel worden gebracht of in gebruik worden gesteld door financiële instellingen waarvoor krachtens het Unierecht inzake financiële diensten vereisten met betrekking tot hun interne governance, regelingen of processen gelden.

AFDELING 2

DELEN VAN INFORMATIE OVER ERNSTIGE INCIDENTEN

Artikel 73

Melding van ernstige incidenten

1. Aanbieders van in de Unie in de handel gebrachte AI-systemen met een hoog risico melden ernstige incidenten bij de markttoezichtautoriteiten van de lidstaten waarin dat incident heeft plaatsgevonden.
2. De in lid 1 bedoelde melding wordt gedaan onmiddellijk nadat de aanbieder een oorzakelijk verband tussen het AI-systeem en het ernstige incident of de redelijke waarschijnlijkheid van een dergelijk verband heeft vastgesteld en in ieder geval uiterlijk 15 dagen nadat de aanbieder of, in voorkomend geval, de gebruiksverantwoordelijke zich bewust wordt van het ernstige incident.

Bij de in de eerste alinea bedoelde meldingstermijn wordt rekening gehouden met de ernst van het ernstige incident.
3. Niettegenstaande lid 2 van dit artikel wordt bij een wijdverbreide inbreuk of een ernstig incident, zoals gedefinieerd in artikel 3, punt 49), b), de in lid 1 van dit artikel bedoelde melding onmiddellijk gedaan, doch uiterlijk twee dagen nadat de aanbieder of, in voorkomend geval, de gebruiksverantwoordelijke zich bewust wordt van dat incident.

4. Niettegenstaande lid 2 wordt bij overlijden van een persoon de melding gedaan onmiddellijk nadat de aanbieder of de gebruiksverantwoordelijke een oorzakelijk verband heeft vastgesteld, of zodra hij of zij dit vermoedt, tussen het AI-systeem met een hoog risico en het ernstige incident, doch uiterlijk tien dagen na de datum waarop de aanbieder of, in voorkomend geval, de gebruiksverantwoordelijke zich bewust wordt van het ernstige incident.
5. Indien dit nodig is om tijdige melding te waarborgen, kan de aanbieder of, in voorkomend geval, de gebruiksverantwoordelijke een eerste, onvolledige, melding doen die wordt gevolgd door een volledige melding.
6. Na de melding van een ernstig incident op grond van lid 1 verricht de aanbieder onverwijld het nodige onderzoek in verband met het ernstige incident en het betrokken AI-systeem. Dit omvat een risicobeoordeling van het incident en corrigerende maatregelen.

De aanbieder werkt tijdens het in de eerste alinea genoemde onderzoek samen met de bevoegde autoriteiten en, in voorkomend geval, met de betrokken aangemelde instantie, en verricht geen onderzoek waarbij het AI-systeem wordt gewijzigd op een wijze die van invloed kan zijn op de latere evaluatie van de oorzaken van het incident, zonder de bevoegde autoriteiten daarvan vooraf in kennis te stellen.

7. Na ontvangst van een melding met betrekking tot een ernstig incident als bedoeld in artikel 3, punt 49, c), stelt de betrokken markttoezichtautoriteit de in artikel 77, lid 1, bedoelde nationale overheidsinstanties of -organen in kennis. De Commissie ontwikkelt specifieke richtsnoeren om nakoming van de in lid 1 van dit artikel vermelde verplichtingen te vergemakkelijken. Die richtsnoeren worden uiterlijk op ... [twaalf maanden na de inwerkingtreding van deze verordening] uitgevaardigd en worden regelmatig geëvalueerd.

8. De markttoezichtautoriteit neemt passende maatregelen, zoals bedoeld in artikel 19 van Verordening (EU) 2019/1020, binnen zeven dagen na de datum waarop zij de in lid 1 van dit artikel bedoelde kennisgeving heeft ontvangen, en volgt de kennisgevings-procedures waarin die verordening voorziet.
9. Voor in bijlage III vermelde AI-systemen met een hoog risico die in de handel zijn gebracht of in gebruik zijn gesteld door aanbieders die onderworpen zijn aan rechtsinstrumenten van de Unie met meldingsverplichtingen die gelijkwaardig zijn aan die van deze verordening, is de melding van ernstige incidenten beperkt tot de in artikel 3, punt 49), c), bedoelde incidenten.
11. Voor AI-systemen met een hoog risico die veiligheidscomponenten van apparaten zijn of zelf apparaten zijn die onder de Verordeningen (EU) 2017/745 en (EU) 2017/746 vallen, wordt de melding van ernstige incidenten beperkt tot de in artikel 3, punt 49, c), van de onderhavige verordening bedoelde incidenten, en wordt het incident gemeld bij de nationale bevoegde autoriteit die daartoe is aangewezen door de lidstaten waar dat incident zich heeft voorgedaan.
11. De nationale bevoegde autoriteiten stellen de Commissie onmiddellijk in kennis van elk ernstig incident, ongeacht of zij al dan niet maatregelen hebben getroffen, overeenkomstig artikel 20 van Verordening (EU) 2019/1020.

AFDELING 3

HANDHAVING

Artikel 74

Markttoezicht op en controle van AI-systemen op de markt van de Unie

1. Verordening (EU) 2019/1020 is van toepassing op AI-systemen die onder deze verordening vallen. Ten behoeve van de doeltreffende handhaving van deze verordening geldt echter het volgende:
 - a) verwijzingen naar een marktdeelnemer krachtens Verordening (EU) 2019/1020 worden begrepen als verwijzingen naar alle in artikel 2, lid 1, van deze verordening geïdentificeerde operators;
 - b) verwijzingen naar een product krachtens Verordening (EU) 2019/1020 worden begrepen als verwijzingen naar alle AI-systemen die binnen het toepassingsgebied van deze verordening vallen.
2. In het kader van hun rapportageverplichtingen krachtens artikel 34, lid 4, van Verordening (EU) 2019/1020 brengen de markttoezichtautoriteiten jaarlijks aan de Commissie en de bevoegde nationale mededingingsautoriteiten verslag uit over alle informatie die in het kader van markttoezichtactiviteiten is verkregen en die van belang kan zijn voor de toepassing van het Unierecht inzake mededingingsregels. Daarnaast brengen zij de Commissie jaarlijks verslag uit over het gebruik van verboden praktijken in de loop van dat jaar en over de maatregelen die genomen zijn.
3. Voor AI-systemen met een hoog risico met betrekking tot producten waarop de in afdeling A van bijlage I vermelde harmonisatiewetgeving van de Unie van toepassing is, is voor de toepassing van deze verordening de markttoezichtautoriteit de autoriteit die verantwoordelijk is voor markttoezichtactiviteiten uit hoofde van die rechtshandelingen.

In afwijking van de eerste alinea kunnen de lidstaten in passende omstandigheden een andere relevante autoriteit aanwijzen om als markttoezichtautoriteit op te treden, mits zij zorgen voor coördinatie met de relevante sectorale markttoezichtautoriteiten die verantwoordelijk zijn voor de handhaving van de in bijlage I vermelde harmonisatiewetgeving van de Unie.

4. De in de artikelen 79 tot en met 83 van deze verordening bedoelde procedures zijn niet van toepassing op AI-systemen die verband houden met producten waarop in de in afdeling A van bijlage I vermelde harmonisatiewetgeving van de Unie van toepassing is, indien de betrokken rechtshandelingen reeds voorzien in procedures die een gelijkwaardig niveau van bescherming waarborgen en hetzelfde doel hebben. In dergelijke gevallen zijn in plaats daarvan de betrokken sectorale procedures van toepassing.
5. Onverminderd de bevoegdheden van markttoezichtautoriteiten krachtens artikel 14 van Verordening (EU) 2019/1020 kunnen markttoezichtautoriteiten met het oog op de doeltreffende handhaving van deze verordening de in artikel 14, lid 4, punten d) en j), van die verordening bedoelde bevoegdheden naargelang van het geval op afstand uitoefenen.
6. Voor AI-systemen met een hoog risico die in de handel worden gebracht, in gebruik worden gesteld of worden gebruikt door financiële instellingen die onder het Unierecht inzake financiële diensten vallen, is de markttoezichtautoriteit voor de toepassing van deze verordening de relevante nationale autoriteit die verantwoordelijk is voor het financiële toezicht op die instellingen krachtens die wetgeving, voor zover het in de handel brengen, in gebruik stellen of gebruik van het AI-systeem rechtstreeks verband houdt met de verlening van die financiële diensten.

7. In afwijking van lid 6 kan in gerechtvaardigde omstandigheden en op voorwaarde dat er coördinatie wordt gewaarborgd, een andere relevante autoriteit door de lidstaat als markttoezichtautoriteit worden aangewezen voor de toepassing van deze verordening.

Nationale markttoezichtautoriteiten die toezicht houden op gereglementeerde kredietinstellingen die onder Richtlijn 2013/36/EU vallen en die deelnemen aan het bij Verordening (EU) nr. 1024/2013 ingestelde gemeenschappelijk toezichtsmechanisme, moeten onverwijld bij de Europese Centrale Bank alle informatie melden die zij bij hun markttoezichtactiviteiten hebben verkregen en die potentieel van belang kan zijn voor de in die verordening nader bepaalde prudentiële-toezichtstaken van de Europese Centrale Bank.

8. Voor AI-systemen met een hoog risico die zijn vermeld in punt 1 van bijlage III, bij deze verordening, voor zover die systemen worden gebruikt voor rechtshandavingsdoeleinden, grenstoezicht en rechtsbedeling en democratie, en voor AI-systemen met een hoog risico die zijn vermeld in de punten 6, 7 en 8 van bijlage III, bij deze verordening wijzen de lidstaten als markttoezichtautoriteiten voor de toepassing van deze verordening hetzij de bevoegde toezichthoudende autoriteiten voor gegevensbescherming krachtens Verordening (EU) 2016/679 of Richtlijn (EU) 2016/680 aan, hetzij een andere autoriteit die is aangewezen onder dezelfde voorwaarden van de artikelen 41 tot en met 44 van Richtlijn (EU) 2016/680. De markttoezichtactiviteiten mogen geenszins afbreuk doen aan de onafhankelijkheid van gerechtelijke instanties of anderszins afbreuk doen aan hun activiteiten wanneer zij optreden in hun gerechtelijke hoedanigheid.

9. Indien instellingen, organen of instanties van de Unie binnen het toepassingsgebied van deze verordening vallen, treedt de Europese Toezichthouder voor gegevensbescherming als hun markttoezichtautoriteit op, behalve ten aanzien van het Hof van Justitie van de Europese Unie in zijn gerechtelijke hoedanigheid.
10. De lidstaten faciliteren de coördinatie tussen krachtens deze verordening aangewezen markttoezichtautoriteiten en andere relevante nationale autoriteiten of instanties die toezicht houden op de toepassing van de in bijlage I vermelde harmonisatiewetgeving van de Unie of andere Unieregels, die mogelijk relevant kunnen zijn voor de in bijlage III vermelde AI-systemen met een hoog risico.
11. Markttoezichtautoriteiten en de Commissie kunnen gezamenlijke activiteiten, waaronder gezamenlijke onderzoeken, voorstellen die door markttoezichtautoriteiten alleen of gezamenlijk met de Commissie moeten worden uitgevoerd, met als doel de naleving te bevorderen, niet-naleving vast te stellen, bewustmaking of richtsnoeren met betrekking tot deze verordening te verstrekken over specifieke categorieën AI-systemen met een hoog risico die in twee of meer lidstaten een ernstig risico blijken te vormen, overeenkomstig artikel 9 van Verordening (EU) 2019/1020. Het AI-bureau draagt zorg voor coördinerende ondersteuning van gezamenlijke onderzoeken.

12. Onverminderd de bevoegdheden krachtens Verordening (EU) 2019/1020, en voor zover relevant en beperkt tot wat nodig is om hun taken uit te voeren, verlenen aanbieders de markttoezichtautoriteiten volledige toegang tot de documentatie en tot de datasets voor het trainen, valideren en testen die worden gebruikt voor de ontwikkeling van AI-systemen met een hoog risico, onder meer, in voorkomend geval en met inachtneming van beveiligingswaarborgen, via applicatieprogramma-interfaces (“API’s”) of andere relevante technische middelen en instrumenten die toegang op afstand mogelijk maken.
13. Markttoezichtautoriteiten wordt toegang tot de broncode van het AI-systeem met een hoog risico verleend op een met redenen omkleed verzoek en uitsluitend als aan beide onderstaande voorwaarden wordt voldaan:
 - a) toegang tot de broncode is noodzakelijk om te beoordelen of een AI-systeem met een hoog risico overeenstemt met de voorschriften van afdeling 2 van hoofdstuk III, en
 - b) de test- of auditprocedures en verificaties op basis van de door de aanbieder verstrekte gegevens en documentatie zijn uitgeput of ontoereikend gebleken.
14. De door de markttoezichtautoriteiten verkregen informatie of documentatie worden verwerkt overeenkomstig de in artikel 78 vastgelegde vertrouwelijkheidsverplichtingen.

Artikel 75

Wederzijdse bijstand, markttoezicht en controle van AI-systemen voor algemene doeleinden

1. Indien een AI-systeem gebaseerd is op een AI-model voor algemene doeleinden en het model en het systeem door dezelfde aanbieder worden ontwikkeld, moet het AI-bureau bevoegd zijn om de naleving van de verplichtingen krachtens deze verordening door dat AI-systeem te monitoren en te bewaken. Om zijn monitoring- en toezichttaken uit te voeren, moet het AI-bureau beschikken over alle in deze afdeling en Verordening (EU) 2019/1020 bepaalde bevoegdheden van een markttoezichtautoriteit.
2. Indien de relevante markttoezichtautoriteiten voldoende reden hebben om van mening te zijn dat AI-systemen voor algemene doeleinden die door gebruiksverantwoordelijken rechtstreeks kunnen worden gebruikt voor ten minste één doel dat op grond van deze verordening naar hoog risico is ingedeeld, niet in overeenstemming zijn met de voorschriften van deze verordening, werken zij samen met het AI-bureau om nalevingsevaluaties te verrichten, en stellen zij de AI-board en andere markttoezichtautoriteiten daarvan in kennis.

3. Indien een markttoezichtautoriteit haar onderzoek naar het AI-systeem met een hoog risico niet kan afronden omdat zij geen toegang heeft tot bepaalde informatie met betrekking tot het AI-model voor algemene doeleinden, hoewel zij al het nodige heeft gedaan om die informatie te verkrijgen, kan zij een met redenen omkleed verzoek indienen bij het AI-bureau, waarmee de toegang tot die informatie wordt afgedwongen. In dat geval verstrekt het AI-bureau de verzoekende autoriteit onverwijld, en in ieder geval binnen dertig dagen, alle informatie die het relevant acht om vast te stellen of een AI-systeem met een hoog risico non-conform is. Markttoezichtautoriteiten waarborgen dat de door hen verkregen informatie overeenkomstig artikel 78 van deze verordening vertrouwelijk wordt behandeld. De procedure van hoofdstuk VI van Verordening (EU) 2019/1020 is van overeenkomstige toepassing.

Artikel 76

Toezicht op tests onder reële omstandigheden door markttoezichtautoriteiten

1. De markttoezichtautoriteiten hebben de bevoegdheden om ervoor te zorgen dat tests onder reële omstandigheden in overeenstemming zijn met deze verordening.
2. Indien AI-systemen waarop toezicht wordt uitgeoefend binnen een AI-testomgeving voor regelgeving krachtens artikel 58, onder reële omstandigheden worden getest, controleren de markttoezichtautoriteiten of artikel 60 wordt nageleefd als onderdeel van hun toezichthoudende rol voor de AI-testomgeving voor regelgeving. Deze autoriteiten kunnen, in voorkomend geval, toestaan dat de aanbieder of potentiële aanbieder in afwijking van de voorwaarden van artikel 60, lid 4, punten f) en g), onder reële omstandigheden test.

3. Een markttoezichtautoriteit die door de aanbieder, de potentiële aanbieder of een derde van een ernstig incident op de hoogte is gebracht of andere redenen heeft om aan te nemen dat niet aan de in de artikelen 60 en 61 bepaalde voorwaarden wordt voldaan, kan op haar grondgebied een van de volgende besluiten nemen, naargelang van het geval:
- a) de tests onder reële omstandigheden opschorten of beëindigen;
 - b) aanbieders of potentiële aanbieders en gebruiksverantwoordelijken of potentiële gebruiksverantwoordelijken voorschrijven dat zij een aspect van de test onder reële omstandigheden wijzigen.
4. Indien een markttoezichtautoriteit een besluit als bedoeld in lid 3 van dit artikel heeft genomen of een bezwaar in de zin van artikel 60, lid 4, punt b), heeft ingediend, worden in het besluit of het bezwaar vermeld wat de redenen daarvoor zijn en onder welke voorwaarden de aanbieder of potentiële aanbieder het besluit of het bezwaar kan aanvechten.
5. Indien, in voorkomend geval, een markttoezichtautoriteit een besluit als bedoeld in lid 3 heeft genomen, deelt zij de redenen daarvoor mee aan de markttoezichtautoriteiten van de andere lidstaten waar het AI-systeem overeenkomstig het testplan is getest.

Artikel 77

Bevoegdheden van de autoriteiten voor de bescherming van de grondrechten

1. Nationale overheidsinstanties of -organen die de nakoming van verplichtingen krachtens Unierecht ter bescherming van grondrechten, waaronder het recht op non-discriminatie, met betrekking tot het gebruik van de in bijlage III vermelde AI-systemen met een hoog risico controleren of handhaven, zijn bevoegd om krachtens deze verordening opgestelde of bijgehouden documentatie in een toegankelijke taal en een toegankelijk formaat aan te vragen en in te zien wanneer toegang tot die documentatie nodig is voor het doeltreffend uitoefenen van de bevoegdheden onder hun mandaat binnen de grenzen van hun rechtsgebied. De overheidsinstantie of het overheidsorgaan in kwestie stelt de markttoezichtautoriteit van de betrokken lidstaat van een dergelijke aanvraag in kennis.
2. Uiterlijk op ... [drie maanden na de inwerkingtreding van deze verordening] stelt elke lidstaat de in lid 1 bedoelde overheidsinstanties of -organen vast en maakt de lijst openbaar. De lidstaten stellen de Commissie en de andere lidstaten in kennis van de lijst en houden deze up-to-date.
3. Indien de in lid 1 bedoelde documentatie ontoereikend is om vast te stellen of sprake is geweest van een inbreuk op verplichtingen krachtens het Unierecht ter bescherming van grondrechten, kunnen de in lid 1 bedoelde overheidsinstanties of -organen een met redenen omkleed verzoek bij de markttoezichtautoriteit indienen om het AI-systeem met een hoog risico met technische middelen te mogen testen. De markttoezichtautoriteit organiseert de testprocedure binnen een redelijke termijn na het verzoek en met nauwe betrokkenheid van de verzoekende overheidsinstantie of het verzoekende overheidsorgaan.

4. Informatie of documentatie die op grond van dit artikel door de in lid 1 van dit artikel bedoelde overheidsinstanties of -organen wordt verkregen, wordt verwerkt overeenkomstig de in artikel 78 beschreven vertrouwelijkheidsverplichtingen.

Artikel 78

Vertrouwelijkheid

1. De Commissie, de markttoezichtautoriteiten en de aangemelde instanties, en alle andere natuurlijke of rechtspersonen die bij de toepassing van deze verordening betrokken zijn, eerbiedigen overeenkomstig het Unierecht of het nationale recht de vertrouwelijke aard van informatie en gegevens die zij hebben verkregen tijdens het uitvoeren van hun taken en activiteiten, met name ter bescherming van:
- a) de intellectuele-eigendomsrechten, en vertrouwelijke bedrijfsinformatie of bedrijfsgeheimen van een natuurlijke of rechtspersoon, waaronder de broncode, uitgezonderd de gevallen bedoeld in artikel 5 van Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad⁵⁷;
 - b) de doeltreffende uitvoering van deze verordening, met name in verband met inspecties, onderzoeken of audits;
 - c) publieke en nationale veiligheidsbelangen;
 - d) het voeren van strafrechtelijke of administratieve procedures;

⁵⁷ Richtlijn (EU) 2016/943 van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (PB L 157 van 15.6.2016, blz. 1).

- e) informatie die op grond van het Unierecht of het nationale recht gerubriceerd is.
2. De autoriteiten die op grond van lid 1 bij de toepassing van deze verordening betrokken zijn, verzoeken alleen om gegevens die strikt noodzakelijk zijn ter beoordeling van het risico van AI-systemen en ter uitoefening van hun bevoegdheden in overeenstemming met deze verordening en met Verordening (EU) 2019/1020. Zij treffen adequate en doeltreffende cyberbeveiligingsmaatregelen ter bescherming van de veiligheid en de vertrouwelijkheid van de verkregen informatie en gegevens en wissen de verzamelde gegevens zodra die niet langer nodig zijn voor het doel waarvoor zij zijn verkregen, overeenkomstig het toepasselijke Unierecht of nationale recht.
3. Onverminderd de leden 1 en 2, mag op vertrouwelijke basis tussen de nationale bevoegde autoriteiten of tussen nationale bevoegde autoriteiten en de Commissie uitgewisselde informatie niet openbaar worden gemaakt zonder voorafgaande raadpleging van de nationale bevoegde autoriteit waarvan de informatie afkomstig is en de gebruiksverantwoordelijke wanneer in punt 1, 6 of 7 van bijlage III vermelde AI-systemen met een hoog risico worden gebruikt door rechtshandavingsinstanties en grenstoezichts-, immigratie- of asielautoriteiten, wanneer die openbaarmaking openbare en nationale veiligheidsbelangen in gevaar zou brengen. Deze informatie-uitwisseling behelst geen gevoelige operationele gegevens in verband met de activiteiten van rechtshandavings-, grenstoezichts-, immigratie- of asielautoriteiten.

Indien de rechtshandhavingsinstanties of immigratie- of asielautoriteiten aanbieders van in punt 1, 6 of 7 van bijlage III bedoelde AI-systemen met een hoog risico zijn, blijft de in bijlage IV vermelde technische documentatie in de gebouwen van die autoriteiten. Die autoriteiten waarborgen dat de in artikel 74, leden 8 en 9, bedoelde markttoezichtautoriteiten zo nodig op verzoek onmiddellijk toegang tot de documentatie kunnen krijgen of een kopie ervan kunnen ontvangen. Alleen personeel van de markttoezichtautoriteit met een passende veiligheidsmachtiging mag die documentatie of kopieën ervan inzien.

4. De leden 1, 2 en 3 laten de rechten en verplichtingen van de Commissie, de lidstaten en hun bevoegde autoriteiten, alsmede die van de aangemelde instanties, met betrekking tot de uitwisseling van informatie en de verspreiding van waarschuwingen, ook in het kader van grensoverschrijdende samenwerking, evenals de verplichtingen van de betrokken partijen om in het kader van het strafrecht van de lidstaten informatie te verstrekken, onverlet.
5. De Commissie en de lidstaten kunnen zo nodig en met inachtneming van de relevante bepalingen van internationale overeenkomsten en handelsakkoorden vertrouwelijke informatie uitwisselen met regelgevingsinstanties van derde landen waarmee zij bilaterale of multilaterale vertrouwelijkheidsovereenkomsten hebben gesloten die een passend niveau van vertrouwelijkheid waarborgen.

Artikel 79

Procedure op nationaal niveau voor de omgang met AI-systemen die een risico vormen

1. Onder AI-systemen die een risico inhouden, worden verstaan “producten die een risico vormen”, zoals gedefinieerd in artikel 3, punt 19, van Verordening (EU) 2019/1020, voor zover die een risico vormen voor de gezondheid, de veiligheid of de grondrechten van personen.

2. Indien de markttoezichtautoriteit van een lidstaat voldoende reden heeft om van mening te zijn dat een AI-systeem een risico vormt, zoals bedoeld in lid 1 van dit artikel, verricht zij een evaluatie van het betrokken AI-systeem ten aanzien van de overeenstemming ervan met alle eisen en verplichtingen van deze verordening. Er wordt bijzondere aandacht besteed aan AI-systemen die een risico vormen voor kwetsbare groepen. Indien er risico's voor de grondrechten worden vastgesteld, stelt de markttoezichtautoriteit tevens de in artikel 77, lid 1, bedoelde relevante nationale overheidsinstanties of -organen in kennis en verleent zij hun haar volledige medewerking. De relevante gebruiksverantwoordelijken werken voor zover noodzakelijk samen met de markttoezichtautoriteit en met de andere in artikel 77, lid 1, bedoelde nationale overheidsinstanties of -organen.

Indien de markttoezichtautoriteit, in voorkomend geval in samenwerking met de in artikel 77, lid 1, bedoelde nationale overheidsinstantie, bij deze evaluatie vaststelt dat het AI-systeem niet aan de eisen en verplichtingen van deze verordening voldoet, gelast zij de betrokken operator zonder onnodige vertraging passende corrigerende maatregelen te nemen om het AI-systeem binnen een termijn die door de markttoezichtautoriteit kan worden vastgesteld, en in elk geval binnen 15 werkdagen of binnen de termijn die is vastgelegd in de van toepassing zijnde relevante harmonisatiewetgeving van de Unie, indien die korter is, conform te maken, uit de handel te nemen of terug te roepen.

De markttoezichtautoriteit stelt de relevante aangemelde instantie daarvan in kennis. Op de in de tweede alinea van dit lid genoemde maatregelen is artikel 18 van Verordening (EU) 2019/1020 van toepassing.

3. Indien de markttoezichtautoriteit van mening is dat de non-conformiteit niet beperkt blijft tot haar nationale grondgebied, brengt zij de Commissie en de andere lidstaten zonder onnodige vertraging op de hoogte van de resultaten van de evaluatie en van de maatregelen die zij de operator heeft opgelegd.
4. De operators zorgen ervoor dat alle betrokken AI-systemen die zij op de Uniemarkt hebben aangeboden aan alle passende corrigerende maatregelen worden onderworpen.
5. Indien de operator van een AI-systeem niet binnen de in lid 2 bedoelde termijn doeltreffende corrigerende actie onderneemt, neemt de markttoezichtautoriteit alle passende voorlopige maatregelen om het op haar nationale markt aanbieden of in gebruik stellen van het AI-systeem te verbieden of te beperken, het product of het op zichzelf staande AI-systeem in de betrokken lidstaat uit de handel te nemen of terug te roepen. Die autoriteit stelt de Commissie en de andere lidstaten zonder onnodige vertraging van deze maatregelen in kennis.
6. De in lid 5 bedoelde kennisgeving omvat alle bekende bijzonderheden, met name de informatie die nodig is om het non-conforme AI-systeem te identificeren en om de oorsprong van het AI-systeem en de toeleveringsketen, de aard van de beweerde non-conformiteit en van het risico, en de aard en de duur van de nationale maatregelen vast te stellen, evenals de argumenten die worden aangevoerd door de betrokken operator. De markttoezichtautoriteiten vermelden met name of de non-conformiteit een of meer van de volgende redenen heeft:
 - a) niet-naleving van het verbod op de in artikel 5 bedoelde AI-praktijken;
 - b) het AI-systeem met een hoog risico voldoet niet aan vereisten van hoofdstuk III, afdeling 2;

- c) tekortkomingen in de in de artikelen 40 en 41 bedoelde geharmoniseerde normen of gemeenschappelijke specificaties die een vermoeden van conformiteit rechtvaardigen;
 - d) niet-naleving van artikel 50.
7. De andere markttoezichtautoriteiten dan de markttoezicht-autoriteit van de lidstaat die de procedure heeft geïnitieerd, brengen de Commissie en de andere lidstaten zonder onnodige vertraging op de hoogte van door hen genomen maatregelen en van aanvullende informatie over de non-conformiteit van het AI-systeem waarover zij beschikken, en van hun bezwaren indien zij het niet eens zijn met de aangemelde nationale maatregel.
8. Indien er binnen drie maanden na ontvangst van de in lid 5 van dit artikel bedoelde kennisgeving door een markttoezichtautoriteit van een lidstaat of door de Commissie geen bezwaar tegen een voorlopige maatregel van een markttoezichtautoriteit van een andere lidstaat is ingediend, wordt die maatregel geacht gerechtvaardigd te zijn. Dit geldt onverminderd de procedurele rechten van de betrokken operator overeenkomstig artikel 18 van Verordening (EU) 2019/1020. De in dit lid bedoelde termijn van drie maanden wordt verkort tot 30 dagen in geval van niet-naleving van het verbod op de in artikel 5 van deze verordening bedoelde AI-praktijken.
9. De markttoezichtautoriteiten zorgen ervoor dat ten aanzien van het betrokken product of AI-systeem zonder onnodige vertraging de passende beperkende maatregelen worden genomen, zoals het uit de handel nemen van het product of het AI-systeem op hun markt.

Artikel 80

Procedure voor de omgang met AI-systemen die conform bijlage III

door de aanbieder zijn ingedeeld als systemen die geen hoog risico met zich meebrengen

1. Indien een markttoezichtautoriteit voldoende reden heeft om van mening te zijn dat een AI-systeem dat door de aanbieder is ingedeeld als een AI-systeem dat geen hoog risico met zich meebrengt op grond van artikel 6, lid 3, wél een hoog risico vormt, toetst zij het betrokken AI-systeem aan de classificatie ervan als AI-systeem met een hoog risico op grond van de voorwaarden van artikel 6, lid 3, en de richtsnoeren van de Commissie.
2. Indien de markttoezichtautoriteit bij die toetsing vaststelt dat het betrokken AI-systeem een hoog risico vormt, eist zij zonder onnodige vertraging van de betrokken aanbieder dat deze alle nodige maatregelen neemt om het AI-systeem in overeenstemming te brengen met de vereisten en verplichtingen van deze verordening, en binnen een termijn die de markttoezichtautoriteit kan voorschrijven passende corrigerende maatregelen neemt.
3. Indien de markttoezichtautoriteit van mening is dat de het gebruik van het AI-systeem niet beperkt blijft tot haar nationale grondgebied, brengt zij de Commissie en de andere lidstaten zonder onnodige vertraging op de hoogte van de resultaten van de toetsing en van de maatregelen die zij de aanbieder heeft opgelegd.

4. De aanbieder zorgt ervoor dat alle nodige maatregelen worden genomen om het AI-systeem in overeenstemming te brengen met de vereisten en verplichtingen van deze verordening. Indien de aanbieder van een betrokken AI-systeem dat AI-systeem niet binnen de in lid 2 van dit artikel bedoelde termijn in overeenstemming brengt met die vereisten en verplichtingen, worden aan de aanbieder overeenkomstig artikel 99 geldboeten opgelegd.
5. De aanbieder zorgt ervoor dat alle betrokken AI-systemen die zij op de Uniemarkt hebben aangeboden aan alle passende corrigerende maatregelen worden onderworpen.
6. Indien de aanbieder van het betrokken AI-systeem niet binnen de in lid 2 van dit artikel bedoelde termijn adequate corrigerende maatregelen neemt, is artikel 79, leden 5 tot en met 9, van toepassing.
7. Indien de markttoezichtautoriteit bij de toetsing op grond van lid 1 van dit artikel vaststelt dat het AI-systeem door de aanbieder ten onrechte als geen hoog risico vormend systeem is ingedeeld om de toepassing van de vereisten van hoofdstuk III, afdeling 2, te omzeilen, worden aan de aanbieder overeenkomstig artikel 99 geldboeten opgelegd.
8. Bij de uitoefening van hun bevoegdheid om op de toepassing van dit artikel toe te zien, en overeenkomstig artikel 11 van Verordening (EU) 2019/1020, kunnen markttoezichtautoriteiten passende controles verrichten waarbij zij met name informatie die is opgeslagen in de in artikel 71 van deze verordening bedoelde EU-databank in aanmerking nemen.

Artikel 81

Vrijwaringsprocedure van de Unie

1. Indien de markttoezichtautoriteit van een lidstaat binnen drie maanden na ontvangst van de in artikel 79, lid 5, bedoelde kennisgeving, of binnen 30 dagen in geval van niet-naleving van het verbod op de in artikel 5 bedoelde AI-praktijken, bezwaar maakt tegen een door een andere markttoezichtautoriteit genomen maatregel, of indien de Commissie de maatregel in strijd acht met het Unierecht, treedt de Commissie zonder onnodige vertraging in overleg met de markttoezichtautoriteit van de betrokken lidstaat en de operator(s), en evalueert zij de nationale maatregel. Op grond van de resultaten van die evaluatie besluit de Commissie binnen zes maanden, of binnen 60 dagen in geval van niet-naleving van het verbod op de in artikel 5 bedoelde AI-praktijken, met ingang van de in artikel 79, lid 5, bedoelde kennisgeving of de nationale maatregel gerechtvaardigd is, en deelt zij haar besluit aan de markttoezichtautoriteit van de betrokken lidstaat mee. De Commissie stelt ook alle andere markttoezichtautoriteiten van haar besluit in kennis.
2. Indien de Commissie de maatregel van de betrokken lidstaat gerechtvaardigd acht, zorgen alle lidstaten ervoor dat zij passende beperkende maatregelen ten aanzien van het betrokken AI-systeem nemen, zoals het zonder onnodige vertraging uit de handel nemen van het AI-systeem op hun markt, en stellen zij de Commissie daarvan in kennis. Indien de Commissie de nationale maatregel ongerechtvaardigd acht, trekt de betrokken lidstaat de maatregel in en stelt hij de Commissie daarvan in kennis.

3. Indien de nationale maatregel gerechtvaardigd wordt geacht en de non-conformiteit van het AI-systeem wordt toegeschreven aan tekortkomingen in de in de artikelen 40 en 41 van deze verordening bedoelde geharmoniseerde normen of gemeenschappelijke specificaties, past de Commissie de procedure van artikel 11 van Verordening (EU) nr. 1025/2012 toe.

Artikel 82

Conforme AI-systemen die een risico inhouden

1. Indien de markttoezichtautoriteit van een lidstaat na uitvoering van een evaluatie overeenkomstig artikel 79 en na raadpleging van de in artikel 77, lid 1, bedoelde relevante nationale overheidsinstantie vaststelt dat een AI-systeem met een hoog risico dat weliswaar voldoet aan deze verordening, toch een risico inhoudt voor de gezondheid of veiligheid van personen, voor de grondrechten of voor andere aspecten van de bescherming van algemene belangen, schrijft zij v de betrokken operator voor dat deze binnen een termijn die zij kan vaststellen, alle passende maatregelen neemt om er zonder onnodige vertraging voor te zorgen dat het betrokken AI-systeem dat risico niet meer inhoudt wanneer het in de handel wordt gebracht of in gebruik wordt gesteld.
2. De aanbieder of andere relevante operator zorgt ervoor dat er binnen de in lid 1 bedoelde door de markttoezichtautoriteit van de lidstaat vastgestelde termijn corrigerende maatregelen worden genomen ten aanzien van alle betrokken AI-systemen die deze op de Uniemarkt heeft aangeboden.

3. De lidstaten brengen de Commissie en de andere lidstaten onmiddellijk op de hoogte van een vaststelling op grond van lid 1. Die informatie omvat alle bekende bijzonderheden, met name de gegevens die nodig zijn om het betrokken AI-systeem te identificeren en om de oorsprong en de toeleveringsketen van het AI-systeem, de aard van het betrokken risico en de aard en de duur van de nationale maatregelen vast te stellen.
4. De Commissie treedt zonder onnodige vertraging in overleg met de betrokken lidstaten en de betrokken operators en evalueert de genomen nationale maatregelen. Aan de hand van die evaluatie besluit de Commissie of de maatregel gerechtvaardigd is, en stelt zij zo nodig andere passende maatregelen voor.
5. De Commissie deelt haar besluit onmiddellijk aan de betrokken lidstaat en de betrokken operators mee. Zij licht ook de andere lidstaten in.

Artikel 83

Formele non-conformiteit

1. Indien de markttoezichtautoriteit van een lidstaat een van de onderstaande feiten vaststelt, schrijft zij de betrokken aanbieder voor dat deze binnen een door haar vast te stellen termijn een einde maakt aan deze non-conformiteit:
 - a) de CE-markering is in strijd met artikel 48 aangebracht;
 - b) er is geen CE-markering aangebracht;
 - c) er is geen in artikel 47 bedoelde EU-conformiteitsverklaring opgesteld;

- d) de in artikel 47 bedoelde EU-conformiteitsverklaring is niet correct opgesteld;
 - e) er heeft geen registratie in de in artikel 71 bedoelde EU-databank plaatsgevonden;
 - f) indien van toepassing, er is geen gemachtigde aangewezen;
 - g) er is geen technische documentatie beschikbaar.
2. Indien de in lid 1 bedoelde non-conformiteit voortduurt, neemt de markttoezichtautoriteit van de betrokken lidstaat passende en evenredige maatregelen om het op de markt aanbieden van het AI-systeem met een hoog risico te beperken of te verbieden, of het AI-systeem onverwijld terug te roepen of uit de handel te nemen.

Artikel 84

Ondersteunende AI-teststructuren van de Unie

1. De Commissie wijst een of meer ondersteunende AI-teststructuren van de Unie aan om op het gebied van AI de in artikel 21, lid 6, van Verordening (EU) 2019/1020 vermelde taken uit te voeren.
2. Onverminderd de in lid 1 bedoelde taken, verstrekken de ondersteunende AI-teststructuren van de Unie ook onafhankelijk technisch of wetenschappelijk advies op verzoek van de AI-board, de Commissie of markttoezichtautoriteiten.

AFDELING 4

RECHTSMIDDELEN

Artikel 85

Recht om een klacht in te dienen bij een markttoezichtautoriteit

Onverminderd andere administratieve of gerechtelijke rechtsmiddelen, kan elke natuurlijke of rechtspersoon die redenen heeft om van mening te zijn dat er inbreuk is gepleegd op de bepalingen van deze verordening, klachten indienen bij de relevante markttoezichtautoriteit.

Overeenkomstig Verordening (EU) 2019/1020 worden dergelijke klachten in aanmerking genomen ter uitvoering van markttoezichtactiviteiten en worden zij behandeld in overeenstemming met de specifieke procedures die de markttoezichtautoriteiten daartoe hebben vastgesteld.

Artikel 86

Recht op uitleg bij individuele besluitvorming

1. Elke getroffen persoon op wie een besluit van toepassing is dat door de gebruiksverantwoordelijke wordt genomen op basis van de output van een in bijlage III vermeld AI-systeem met een hoog risico, met uitzondering van systemen die in punt 2 van die bijlage zijn vermeld, en dat rechtsgevolgen heeft voor die persoon, of op deze op vergelijkbare wijze aanzienlijke invloed heeft die hij of zij als nadelige gevolgen voor zijn of haar gezondheid, veiligheid of grondrechten beschouwt, heeft het recht om van de gebruiksverantwoordelijke duidelijke, inhoudelijke uitleg te verkrijgen bij de rol van het AI-systeem in de besluitvormingsprocedure en de voornaamste elementen van het genomen besluit.

2. Lid 1 is niet van toepassing op het gebruik van AI-systemen waarvoor uitzonderingen op of beperkingen van de verplichting krachtens dat lid voortvloeien uit het Unierecht of het nationale recht in naleving van het Unierecht.
3. Dit artikel is enkel van toepassing voor zover het Unierecht niet anderszins in het in lid 1 bedoelde recht voorziet.

Artikel 87

Melding van inbreuken en bescherming van melders

Richtlijn (EU) 2019/1937 is van toepassing op het melden van inbreuken op deze verordening en op de bescherming van personen die dergelijke inbreuken melden.

AFDELING 5

TOEZICHT, ONDERZOEK, HANDHAVING EN MONITORING

TEN AANZIEN VAN AANBIEDERS VAN AI-MODELLEN VOOR ALGEMENE DOELEINDEN

Artikel 88

Handhaving van de verplichtingen van aanbieders van AI-modellen voor algemene doeleinden

1. De Commissie heeft exclusieve bevoegdheden voor toezicht op en handhaving van hoofdstuk V, rekening houdend met de procedurele waarborgen krachtens artikel 94. De Commissie belast het AI-bureau met de uitvoering van deze taken, onverminderd de organisatiebevoegdheden van de Commissie en de bevoegdheidsverdeling tussen de lidstaten en de Unie op grond van de Verdragen.

2. Onverminderd artikel 75, lid 3, kunnen markttoezichtautoriteiten de Commissie verzoeken de in deze afdeling vastgestelde bevoegdheden uit te oefenen indien dat noodzakelijk en evenredig is om te helpen bij de uitvoering van hun taken krachtens deze verordening.

Artikel 89

Monitoringmaatregelen

1. Voor de uitvoering van de taken die hem uit hoofde van deze afdeling zijn toegewezen, kan het AI-bureau de nodige maatregelen nemen de daadwerkelijke uitvoering en naleving van deze verordening, inclusief hun inachtneming van goedgekeurde praktijkcodes, door aanbieders van AI-modellen voor algemene doeleinden te monitoren.
2. Aanbieders verder in de AI-waardeketen hebben het recht een klacht in te dienen wegens inbreuk op deze verordening. Klachten moeten terdege worden gemotiveerd en moeten ten minste het volgende vermelden of bevatten:
 - a) het contactpunt van de aanbieder van het betrokken AI-model voor algemene doeleinden;
 - b) een beschrijving van de relevante feiten, de desbetreffende bepalingen van deze verordening en de reden waarom de aanbieder verder in de AI-waardeketen van mening is dat de aanbieder van het betrokken AI-model voor algemene doeleinden inbreuk op deze verordening heeft gemaakt;
 - c) alle overige informatie die de aanbieder verder in de AI-waardeketen die het verzoek heeft ingediend, relevant acht, in voorkomend geval ook op eigen initiatief verzamelde informatie.

Artikel 90

Waarschuwingen voor systeemrisico's door het wetenschappelijk panel

1. Het wetenschappelijk panel kan het AI-bureau een gekwalificeerde waarschuwing geven indien het redenen heeft om te vermoeden dat:
 - a) een AI-model voor algemene doeleinden een concreet aanwijsbaar risico op Unieniveau vormt, of
 - b) een AI-model voor algemene doeleinden aan de in artikel 51 bedoelde voorwaarden beantwoordt.
2. Naar aanleiding van een dergelijke gekwalificeerde waarschuwing kan de Commissie via het AI-Bureau, na de AI-board in kennis gesteld te hebben, de in deze afdeling vastgelegde bevoegdheden uitoefenen om de aangelegenheid te beoordelen. Het AI-bureau stelt de AI-board in kennis van elke maatregel overeenkomstig de artikelen 91 tot en met 94.
3. Gekwalificeerde waarschuwingen moeten terdege worden gemotiveerd en ten minste het volgende vermelden of bevatten:
 - a) het contactpunt van de aanbieder van het betrokken AI-model voor algemene doeleinden dat een systeemrisico vormt;
 - b) een beschrijving van de relevante feiten en de redenen voor de waarschuwing door het wetenschappelijk panel;
 - c) alle overige informatie die het wetenschappelijk panel relevant acht, in voorkomend geval ook op eigen initiatief verzamelde informatie.

Artikel 91

Bevoegdheid om documentatie en informatie op te vragen

1. De Commissie kan de aanbieder van het betrokken AI-model voor algemene doeleinden verzoeken de door de aanbieder overeenkomstig de artikelen 53 en 55 opgestelde documentatie of eventuele aanvullende informatie te verstrekken die nodig is om te beoordelen of hij deze verordening naleeft.
2. Alvorens het verzoek om informatie te verzenden, kan het AI-bureau een gestructureerde dialoog met de aanbieder van het AI-model voor algemene doeleinden aangaan.
3. Op een terdege gemotiveerd verzoek van het wetenschappelijk panel kan de Commissie een verzoek om informatie tot een aanbieder van een AI-model voor algemene doeleinden richten, indien de toegang tot informatie noodzakelijk en evenredig is voor de uitvoering van de taken van het wetenschappelijk panel op grond van artikel 68, lid 2.
4. Het verzoek om informatie vermeldt de rechtsgrondslag en het doel van het verzoek, om wat voor informatie wordt verzocht, de termijn waarbinnen de informatie moet worden verstrekt, en de in artikel 101 bepaalde geldboeten voor het verstrekken van onjuiste, onvolledige of misleidende informatie.

5. De aanbieders van het betrokken AI-model voor algemene doeleinden of hun vertegenwoordiger verstrekken de gevraagde informatie. In het geval van rechtspersonen, bedrijven of firma's, of indien de aanbieder geen rechtspersoonlijkheid heeft, verstrekken de personen die krachtens de wet of hun statuten gemachtigd zijn om hen te vertegenwoordigen, de gevraagde informatie namens de aanbieder van het betrokken AI-model voor algemene doeleinden. De informatie kan door naar behoren gemachtigde advocaten namens hun cliënten worden verstrekt. De cliënten blijven niettemin volledig verantwoordelijk indien de verstrekte informatie onvolledig, onjuist of misleidend is.

Artikel 92

Bevoegdheid voor het verrichten van evaluaties

1. Het AI-bureau kan na raadpleging van de AI-board evaluaties van het betrokken AI-model voor algemene doeleinden verrichten teneinde:
- a) te beoordelen of de aanbieder voldoet aan de verplichtingen van deze verordening indien de op grond van artikel 91 verzamelde informatie ontoereikend is, of
 - b) onderzoek te doen naar systeemrisico's op Unieniveau van AI-modellen voor algemene doeleinden met systeemrisico's, met name naar aanleiding van een gekwalificeerde melding van het wetenschappelijk panel overeenkomstig artikel 90, lid 1, punt a).
2. De Commissie kan besluiten om, onder meer uit het krachtens artikel 68 opgericht wetenschappelijk panel, onafhankelijke deskundigen aan te wijzen om namens haar evaluaties te verrichten. Voor deze taak aangewezen onafhankelijke deskundigen moeten voldoen aan de criteria van artikel 68, lid 2.

3. Voor de toepassing van lid 1 kan de Commissie verzoeken om toegang tot het betrokken AI-model voor algemene doeleinden via API's of andere passende technische middelen en instrumenten, waaronder de broncode.
4. Het verzoek om informatie vermeldt de rechtsgrondslag en het doel en de redenen van het verzoek, de termijn waarbinnen de toegang moet worden verleend, en de in artikel 101 bepaalde geldboeten voor het niet bieden van toegang.
5. De aanbieders van AI-modellen voor algemene doeleinden of hun vertegenwoordiger verstrekken de gevraagde informatie. In het geval van rechtspersonen, bedrijven of firma's of indien de aanbieder geen rechtspersoonlijkheid heeft, verlenen de personen die krachtens de wet of hun statuten gemachtigd zijn om hen te vertegenwoordigen, de gevraagde toegang namens de aanbieder van het betrokken AI-model voor algemene doeleinden.
6. De Commissie stelt uitvoeringshandelingen vast met de gedetailleerde regelingen en voorwaarden voor de evaluaties, met inbegrip van de gedetailleerde regelingen voor het betrekken van onafhankelijke deskundigen, en de selectieprocedure daarvoor. Die uitvoeringshandelingen worden volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure vastgesteld.
7. Alvorens om toegang tot het betrokken AI-model voor algemene doeleinden te verzoeken, kan het AI-bureau een gestructureerde dialoog met de aanbieder van het AI-model voor algemene doeleinden aangaan om meer informatie te verzamelen over de interne tests van het model, de interne waarborgen ter voorkoming van systeemrisico's en andere interne procedures en maatregelen die de aanbieder heeft genomen om dergelijke risico's te beperken.

Artikel 93

Bevoegdheid voor het verzoeken om maatregelen

1. Indien nodig en passend kan de Commissie aanbieders erom verzoeken:
 - a) passende maatregelen te nemen om te voldoen aan de verplichtingen van de artikelen 53 en 54;
 - b) risicobeperkende maatregelen te nemen indien de overeenkomstig artikel 92 verrichte evaluatie aanleiding heeft gegeven tot ernstige en concrete aanwijzingen voor een systeemrisico op Unieniveau;
 - c) het op de markt aanbieden van het model te beperken, dan wel het uit de handel te nemen of terug te roepen.
2. Alvorens om een maatregel te verzoeken kan het AI-bureau een gestructureerde dialoog met de aanbieder van het AI-model voor algemene doeleinden aangaan.
3. Indien de aanbieder van het AI-model voor algemene doeleinden dat een systeemrisico vormt, tijdens de in lid 2 bedoelde gestructureerde dialoog toezeggingen doet om risicobeperkende maatregelen uit te voeren om een systeemrisico op Unieniveau aan te pakken, kan de Commissie die toezeggingen bij besluit bindend maken en verklaren dat er geen verdere gronden voor actie zijn.

Artikel 94

Procedurele rechten van marktdeelnemers die het AI-model voor algemene doeleinden aanbieden

Artikel 18 van Verordening (EU) 2019/1020 is van overeenkomstige toepassing op de aanbieders van het AI-model voor algemene doeleinden, onverminderd specifiekere procedurele rechten waarin deze verordening voorziet.

Hoofdstuk X

Gedragcodes en richtsnoeren

Artikel 95

Gedragcodes voor vrijwillige toepassing van specifieke voorschriften

1. Het AI-bureau en de lidstaten stimuleren en faciliteren de opstelling van gedragcodes, met inbegrip van gerelateerde governancemechanismen, die bedoeld zijn om de vrijwillige toepassing van sommige of alle voorschriften van hoofdstuk III, afdeling 2, op andere AI-systemen dan AI-systemen met een hoog risico te bevorderen, rekening houdend met de beschikbare technische oplossingen en beste praktijken van de sector die de toepassing van dergelijke voorschriften mogelijk maken.

2. Het AI-bureau en de lidstaten faciliteren de opstelling van gedragscodes met betrekking tot de vrijwillige toepassing, onder meer door gebruiksverantwoordelijken, van specifieke voorschriften voor alle AI-systemen, op basis van duidelijke doelstellingen en kernprestatie-indicatoren om de verwezenlijking van die doelstellingen te meten, met inbegrip van elementen zoals, maar niet beperkt tot:
- a) toepasselijke elementen waarin de ethische richtsnoeren van de Unie voor betrouwbare AI voorzien;
 - b) het beoordelen en tot een minimum beperken van het effect van AI-systemen op de milieuduurzaamheid, onder meer wat betreft energie-efficiënte programmering en technieken voor het op efficiënte wijze ontwerpen, trainen en gebruiken van AI;
 - c) het bevorderen van AI-geletterdheid, met name die van personen die te maken hebben met de ontwikkeling, de werking en het gebruik van AI;
 - d) het faciliteren van een inclusief en divers ontwerp van AI-systemen, onder meer door de oprichting van inclusieve en diverse ontwikkelingsteams en de bevordering van de deelname van belanghebbenden aan dat proces;
 - e) het beoordelen en voorkomen van de negatieve gevolgen van AI-systemen voor kwetsbare personen of groepen van kwetsbare personen, ook wat betreft de toegankelijkheid voor personen met een handicap, en voor gendergelijkheid.

3. Gedragscodes kunnen door individuele aanbieders of gebruiksverantwoordelijken van AI-systemen of door organisaties die hen vertegenwoordigen, of allebei, worden opgesteld, ook met betrokkenheid van geïnteresseerde belanghebbenden en hun representatieve organisaties, met inbegrip van maatschappelijke organisaties en de academische wereld. Gedragscodes kunnen betrekking hebben op een of meer AI-systemen, gelet op de gelijkenis qua beoogd doel van de betrokken systemen.
4. Het AI-bureau en de lidstaten houden rekening met de specifieke belangen en behoeften van kmo's, waaronder start-ups, bij het stimuleren en faciliteren van het opstellen van gedragscodes.

Artikel 96

Richtsnoeren van de Commissie over de uitvoering van deze verordening

1. De Commissie ontwikkelt richtsnoeren over de praktische uitvoering van deze verordening, en met name over:
 - a) de toepassing van de in de artikelen 8 tot en met 15 en artikel 25 bedoelde vereisten en verplichtingen;
 - b) de in artikel 5 bedoelde verboden praktijken;
 - c) de praktische uitvoering van de bepalingen in verband met substantiële wijziging;
 - d) de praktische uitvoering van de in artikel 50 vastgelegde transparantieplichtingen;

- e) gedetailleerde informatie over het verband van deze verordening met de in bijlage I vermelde harmonisatiewetgeving van de Unie en met andere relevante onderdelen van het Unierecht, onder meer wat betreft de consistentie bij de handhaving ervan;
- f) de toepassing van de definitie van een AI-systeem als gedefinieerd in artikel 3, punt 1).

Bij het uitvaardigen van dergelijke richtsnoeren besteedt de Commissie bijzondere aandacht aan de behoeften van kmo's, met inbegrip van start-ups, lokale overheidsinstanties en sectoren die het waarschijnlijkst door deze verordening zullen worden beïnvloed.

In de in de eerste alinea van dit lid bedoelde richtsnoeren wordt terdege rekening gehouden met de algemeen erkende stand van de techniek op het gebied van AI en met de relevante in de artikelen 40 en 41 bedoelde geharmoniseerde normen en gemeenschappelijke specificaties, dan wel met de krachtens de harmonisatiewetgeving van de Unie vastgestelde geharmoniseerde normen of technische specificaties.

2. Op verzoek van de lidstaten of het AI-bureau of op eigen initiatief actualiseert de Commissie eerder vastgestelde richtsnoeren wanneer dit nodig wordt geacht.

Hoofdstuk XI

Bevoegdheidsdelegatie en comitéprocedure

Artikel 97

Uitoefening van de bevoegdheidsdelegatie

1. De bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend onder de in dit artikel neergelegde voorwaarden.
2. De in artikel 6, leden 6 en 7, artikel 7, leden 1 en 3, artikel 11, lid 3, artikel 43, leden 5 en 6, artikel 47, lid 5, artikel 51, lid 3, artikel 52, lid 4, en artikel 53, leden 5 en 6, bedoelde bevoegdheid om gedelegeerde handelingen vast te stellen, wordt aan de Commissie toegekend voor een termijn van vijf jaar met ingang van ... [de datum van inwerkingtreding van deze verordening]. De Commissie stelt uiterlijk negen maanden voor het einde van de termijn van vijf jaar een verslag op over de bevoegdheidsdelegatie. De bevoegdheidsdelegatie wordt stilzwijgend met termijnen van dezelfde duur verlengd, tenzij het Europees Parlement of de Raad zich uiterlijk drie maanden voor het einde van elke termijn tegen deze verlenging verzet.
3. Het Europees Parlement of de Raad kan de in artikel 6, leden 6 en 7, artikel 7, leden 1 en 3, artikel 11, lid 3, artikel 43, leden 5 en 6, artikel 47, lid 5, artikel 51, lid 3, artikel 52, lid 4, en artikel 53, leden 5 en 6, bedoelde bevoegdheidsdelegatie te allen tijde intrekken. Het besluit tot intrekking beëindigt de delegatie van de in dat besluit genoemde bevoegdheid. Het wordt van kracht op de dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie* of op een daarin genoemde latere datum. Het laat de geldigheid van de reeds van kracht zijnde gedelegeerde handelingen onverlet.

4. Vóór de vaststelling van een gedelegeerde handeling raadpleegt de Commissie de door elke lidstaat aangewezen deskundigen overeenkomstig de beginselen die zijn neergelegd in het Interinstitutioneel Akkoord van 13 april 2016 over beter wetgeven.
5. Zodra de Commissie een gedelegeerde handeling heeft vastgesteld, doet zij daarvan gelijktijdig kennisgeving aan het Europees Parlement en de Raad.
6. Een op grond van artikel 6, lid 6 of 7, artikel 7, lid 1 of 3, artikel 11, lid 3, artikel 43, lid 5 of 6, artikel 47, lid 5, artikel 51, lid 3, artikel 52, lid 4, of artikel 53, lid 5 of 6, vastgestelde gedelegeerde handeling treedt alleen in werking indien het Europees Parlement noch de Raad daartegen binnen een termijn van drie maanden na de kennisgeving van de handeling aan het Europees Parlement en de Raad bezwaar heeft gemaakt, of indien zowel het Europees Parlement als de Raad voor het verstrijken van die termijn de Commissie hebben meegedeeld dat zij daartegen geen bezwaar zullen maken. Die termijn wordt op initiatief van het Europees Parlement of de Raad met drie maanden verlengd.

Artikel 98

Comitéprocedure

1. De Commissie wordt bijgestaan door een comité. Dat comité is een comité in de zin van Verordening (EU) nr. 182/2011.
2. Wanneer naar dit lid wordt verwezen, is artikel 5 van Verordening (EU) nr. 182/2011 van toepassing.

Hoofdstuk XII

Sancties

Artikel 99

Sancties

1. Overeenkomstig de voorwaarden van deze verordening stellen de lidstaten de voorschriften vast voor sancties en andere handhavingsmaatregelen, die ook waarschuwingen en niet-monetaire maatregelen kunnen omvatten, die van toepassing zijn op inbreuken op deze verordening door operatoren, en nemen zij alle nodige maatregelen om ervoor te zorgen dat deze naar behoren en doeltreffend worden uitgevoerd, daarbij rekening houdend met de richtsnoeren die de Commissie op grond van artikel 96 heeft uitgevaardigd. De sancties moeten doeltreffend, evenredig en afschrikkend zijn. Hierbij wordt rekening gehouden met de belangen van kmo's, met inbegrip van start-ups, en hun economische levensvatbaarheid.
2. De lidstaten stellen de Commissie onverwijld en uiterlijk op de datum van toepassing in kennis van de in lid 1 bedoelde voorschriften voor sancties en andere handhavingsmaatregelen en delen haar onverwijld alle latere wijzigingen daarvan mee.
3. Voor de niet-naleving van het verbod op de in artikel 5 bedoelde AI-praktijken gelden administratieve geldboeten tot 35 000 000 EUR of, indien de overtreder een onderneming is, tot 7 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, indien dat hoger is.

4. Voor de niet-naleving van een van de volgende bepalingen in verband met operatoren of aangemelde instanties, uitgezonderd die welke zijn neergelegd in artikel 5, gelden administratieve geldboeten tot 15 000 000 EUR of, indien de overtreder een onderneming is, tot 3 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, indien dat hoger is:
- a) verplichtingen voor aanbieders op grond van artikel 16;
 - b) verplichtingen voor gemachtigden op grond van artikel 22;
 - c) verplichtingen voor importeurs op grond van artikel 23;
 - d) verplichtingen voor distributeurs op grond van artikel 24;
 - e) verplichtingen voor gebruiksverantwoordelijken op grond van artikel 26;
 - f) eisen en verplichtingen voor aangemelde instanties op grond van artikel 31, artikel 33, lid 1, 3 of 4, of artikel 34;
 - g) transparantieplichtingen voor aanbieders en gebruiksverantwoordelijken op grond van artikel 50.
5. Voor de verstrekking van onjuiste, onvolledige of misleidende informatie aan aangemelde instanties of nationale bevoegde autoriteiten naar aanleiding van een verzoek, gelden administratieve geldboeten tot 7 500 000 EUR of, indien de overtreder een onderneming is, tot 1 % van haar totale wereldwijde jaarlijkse omzet voor het voorafgaande boekjaar, indien dat hoger is.
6. In het geval van kmo's, met inbegrip van start-ups, komt elke in dit artikel bedoelde boete neer op de percentages of, indien dat lager is, het bedrag als bedoeld in de leden 3, 4 en 5.

7. Bij het besluiten om al dan niet een administratieve geldboete op te leggen en bij het bepalen van het bedrag van de administratieve geldboete in elk individueel geval worden alle relevante omstandigheden van de specifieke situatie in aanmerking genomen en wordt naargelang van het geval rekening gehouden met het volgende:
- a) de aard, ernst en duur van de inbreuk en de gevolgen ervan, rekening houdend met het doel van het AI-systeem en, indien passend, het aantal getroffen personen en de omvang van de door hen geleden schade;
 - b) of administratieve geldboeten reeds door andere markttoezichtautoriteiten voor dezelfde inbreuk op dezelfde operator zijn toegepast;
 - c) of administratieve geldboeten reeds door andere autoriteiten op dezelfde operator zijn toegepast voor inbreuken op andere bepalingen van het Unierecht of van nationaal recht, wanneer dergelijke inbreuken het resultaat zijn van hetzelfde handelen of nalaten dat een relevante inbreuk op deze verordening vormt;
 - d) de omvang, de jaaromzet en het marktaandeel van de operator die de inbreuk pleegt;
 - e) elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien;
 - f) de mate waarin er met de nationale bevoegde autoriteiten is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;

- g) de mate waarin de operator verantwoordelijk is, rekening houdend met de technische en organisatorische maatregelen die hij heeft genomen;
 - h) de wijze waarop de nationale bevoegde autoriteiten kennis hebben gekregen van de inbreuk, met name of, en zo ja in hoeverre, de operator de inbreuk heeft gemeld;
 - i) de opzettelijke of nalatige aard van de inbreuk;
 - j) door de operator genomen maatregelen om de door de getroffen personen geleden schade te beperken.
8. Elke lidstaat stelt regels vast betreffende de vraag in hoeverre administratieve geldboeten kunnen worden opgelegd aan in die lidstaat gevestigde overheidsinstanties of -organen.
9. Afhankelijk van het rechtstelsel van de lidstaten kunnen de regels voor administratieve geldboeten zodanig worden toegepast dat de boeten worden opgelegd door bevoegde nationale rechters of andere instanties, naargelang van het geval in die lidstaten. De toepassing van zulke regels in die lidstaten heeft een gelijkwaardig effect.
10. De uitoefening van bevoegdheden uit hoofde van dit artikel is onderworpen aan passende procedurele waarborgen overeenkomstig het Unierecht en het nationale recht, waaronder een doeltreffende voorziening in rechte en een eerlijke rechtsbedeling.
11. De lidstaten brengen jaarlijks verslag uit aan de Commissie over de administratieve geldboeten die zij in de loop van dat jaar overeenkomstig dit artikel hebben opgelegd, en over alle daarmee verband houdende geschil- of gerechtelijke procedures.

Artikel 100

Administratieve geldboeten voor instellingen, organen en instanties van de Unie

1. De Europese Toezichthouder voor gegevensbescherming kan administratieve geldboeten opleggen aan instellingen, organen en instanties van de Unie die binnen het toepassingsgebied van deze verordening vallen. Bij het besluiten om al dan niet een administratieve geldboete op te leggen en het bepalen van het bedrag van de administratieve geldboete in elk individueel geval worden alle relevante omstandigheden van de specifieke situatie in aanmerking genomen en wordt terdege rekening gehouden met het volgende:
 - a) de aard, ernst en duur van de inbreuk en de gevolgen ervan, rekening houdend met het doel van het AI-systeem in kwestie, alsmede, waar dit passend is, het aantal getroffen personen en de omvang van de door hen geleden schade;
 - b) de mate van verantwoordelijkheid van de instelling, het orgaan of de instantie van de Unie, rekening houdend met de technische en organisatorische maatregelen die zij hebben genomen;
 - c) maatregelen die de instelling, het orgaan of de instantie van de Unie heeft genomen om de door de getroffen personen geleden schade te beperken;
 - d) de mate van samenwerking met de Europese Toezichthouder voor gegevensbescherming om de inbreuk te verhelpen en de mogelijke nadelige gevolgen van de inbreuk te beperken, waaronder naleving van eventuele maatregelen die eerder door de Europese Toezichthouder voor gegevensbescherming ten aanzien van dezelfde kwestie aan de instelling, het orgaan of de instantie in kwestie van de Unie zijn opgelegd;

- e) soortgelijke eerdere inbreuken door de instelling, het orgaan of de instantie van de Unie;
 - f) de wijze waarop de Europese Toezichthouder voor gegevensbescherming kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de instelling, het orgaan of de instantie van de Unie de inbreuk heeft gemeld;
 - g) de jaarlijkse begroting van de instelling, het orgaan of de instantie van de Unie.
- 2. Voor de niet-naleving van het verbod op de in artikel 5 bedoelde AI-praktijken gelden administratieve geldboeten tot 1 500 000 EUR.
 - 3. Voor de non-conformiteit van het AI-systeem met eisen of verplichtingen krachtens deze verordening, uitgezonderd die bepaald in artikel 5, gelden administratieve geldboeten tot 750 000 EUR.
 - 4. Alvorens een besluit op grond van dit artikel te nemen, stelt de Europese Toezichthouder voor gegevensbescherming de instelling, het orgaan of de instantie van de Unie ten aanzien waarvan hij een procedure voert, in de gelegenheid om te worden gehoord over de mogelijke inbreuk. De Europese Toezichthouder voor gegevens-bescherming baseert zijn besluiten uitsluitend op elementen en omstandigheden waarover de betrokken partijen opmerkingen hebben kunnen maken. Eventuele indieners van klachten worden nauw betrokken bij de procedure.

5. Het recht van verdediging van de partijen wordt in de loop van de procedure ten volle geëerbiedigd. Zij hebben recht op toegang tot het dossier van de Europese Toezichthouder voor gegevensbescherming, onder voorbehoud van het gerechtvaardigde belang van andere natuurlijke personen of ondernemingen bij de bescherming van hun persoonsgegevens of bedrijfsgeheimen.
6. De bedragen die worden geïnd door het opleggen van de geldboeten van dit artikel, dragen bij aan de algemene begroting van de Unie. De geldboeten doen geen afbreuk aan de doeltreffende werking van de instelling, het orgaan of de instantie van de Unie waaraan een geldboete is opgelegd.
7. De Europese Toezichthouder voor gegevensbescherming stelt de Commissie jaarlijks in kennis van de administratieve geldboeten die hij op grond van dit artikel heeft opgelegd en van alle geschil- of gerechtelijke procedures die hij heeft ingeleid.

Artikel 101

Geldboeten voor aanbieders van AI-systemen voor algemene doeleinden

1. De Commissie kan aanbieders van AI-modellen voor algemene doeleinden geldboeten opleggen van ten hoogste 3 % van hun jaarlijkse totale wereldwijde omzet in het voorgaande boekjaar of 15 000 000 EUR, indien dat hoger is, wanneer de Commissie vaststelt dat de aanbieder opzettelijk of uit onachtzaamheid:
 - a) inbreuk heeft gepleegd op de desbetreffende bepalingen van deze verordening;
 - b) niet heeft voldaan aan een verzoek om een document of om informatie op grond van artikel 91, of onjuiste, onvolledige of misleidende informatie heeft verstrekt;

- c) een op grond van artikel 93 gevraagde maatregel niet heeft nageleefd;
- d) de Commissie geen toegang tot het AI-model voor algemene doeleinden of het AI-model voor algemene doeleinden met een systeemrisico heeft gegeven voor de doeleinden van de evaluatie op grond van artikel 92.

Bij de vaststelling van het bedrag van de geldboete of de dwangsom wordt met de aard, de ernst en de duur van de inbreuk rekening gehouden, met inachtneming van de beginselen van evenredigheid en redelijkheid. De Commissie houdt ook rekening met verbintenissen die zijn aangegaan overeenkomstig artikel 93, lid 3, of die zijn aangegaan in relevante praktijkcodes overeenkomstig artikel 56.

- 2. Alvorens het besluit op grond van lid 1 vast te stellen, deelt de Commissie haar voorlopige bevindingen mee aan de aanbieder van het AI-model voor algemene doeleinden, en stelt zij hem in de gelegenheid te worden gehoord.
- 3. De overeenkomstig dit artikel opgelegde geldboeten zijn doeltreffend, evenredig en afschrikkend.
- 4. Informatie over geldboeten die uit hoofde van dit artikel zijn opgelegd, wordt in voorkomend geval ook aan de AI-board meegedeeld.
- 5. Het Hof van Justitie van de Europese Unie heeft volledige rechtsmacht ter zake van beroep tegen besluiten waarbij de Commissie krachtens dit artikel een geldboete vaststelt. Het kan de opgelegde geldboete vernietigen, verlagen of verhogen.

6. De Commissie stelt uitvoeringshandelingen vast met gedetailleerde regelingen en procedurele waarborgen voor procedures met het oog op de eventuele vaststelling van besluiten op grond van lid 1 van dit artikel. Die uitvoeringshandelingen worden vastgesteld volgens de in artikel 98, lid 2, bedoelde onderzoeksprocedure.

Hoofdstuk XIII

Slotbepalingen

Artikel 102

Wijziging van Verordening (EG) nr. 300/2008

Aan artikel 4, lid 3, van Verordening (EG) nr. 300/2008 wordt de volgende alinea toegevoegd:

“Bij het vaststellen van gedetailleerde maatregelen met betrekking tot technische specificaties en procedures voor de goedkeuring en het gebruik van veiligheidsuitrusting betreffende artificiële-intelligentiesystemen in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,+}, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 103

Wijziging van Verordening (EU) nr. 167/2013

Aan artikel 17, lid 5, van Verordening (EU) nr. 167/2013 wordt de volgende alinea toegevoegd:

“Bij het vaststellen van gedelegeerde handelingen krachtens de eerste alinea betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,+}, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 104

Wijziging van Verordening (EU) nr. 168/2013

Aan artikel 22, lid 5, van Verordening (EU) nr. 168/2013 wordt de volgende alinea toegevoegd:

“Bij het vaststellen van gedelegeerde handelingen krachtens de eerste alinea betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,+}, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 105

Wijziging van Richtlijn 2014/90/EU

Aan artikel 8 van Richtlijn 2014/90/EU wordt het volgende lid toegevoegd:

- “5. Voor artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,+}, neemt de Commissie bij het uitvoeren van haar activiteiten krachtens lid 1 en bij het vaststellen van technische specificaties en testnormen overeenkomstig de leden 2 en 3 de eisen van hoofdstuk III, hoofdstuk 2, van die verordening in aanmerking.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 106

Wijziging van Richtlijn (EU) 2016/797

Aan artikel 5 van Richtlijn (EU) 2016/797 wordt het volgende lid toegevoegd:

- “12. Bij het vaststellen van gedelegeerde handelingen krachtens lid 1 en uitvoeringshandelingen krachtens lid 11 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad⁺, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 107
Wijziging van Verordening (EU) 2018/858

Aan artikel 5 van Verordening (EU) 2018/858 wordt het volgende lid toegevoegd:

- “4. “Bij het vaststellen van gedelegeerde handelingen krachtens lid 3 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,+}, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 108
Wijzigingen van Verordening (EU) 2018/1139

Verordening (EU) 2018/1139 wordt als volgt gewijzigd:

1) aan artikel 17 wordt het volgende lid toegevoegd:

“3. Onverminderd lid 2 worden bij het vaststellen van uitvoeringshandelingen krachtens lid 1 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,} de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”;

2) aan artikel 19 wordt het volgende lid toegevoegd:

“4. Bij het vaststellen van gedelegeerde handelingen krachtens de leden 1 en 2 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/...⁺⁺, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.”;

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

⁺⁺ PB: gelieve het nummer van deze verordening in te vullen (2021/0106(COD)).

3) aan artikel 43 wordt het volgende lid toegevoegd:

“4. Bij het vaststellen van uitvoeringshandelingen krachtens lid 1 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/...⁺, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.”;

4) aan artikel 47 wordt het volgende lid toegevoegd:

“3. Bij het vaststellen van gedelegeerde handelingen krachtens de leden 1 en 2 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/...⁺, worden de eisen van titel hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.”;

5) aan artikel 57 wordt de volgende alinea toegevoegd:

“Bij het vaststellen van die uitvoeringshandelingen betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/...⁺, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.”;

6) aan artikel 58 wordt het volgende lid toegevoegd:

“3. Bij het vaststellen van gedelegeerde handelingen krachtens de leden 1 en 2 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/...⁺, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.”.

⁺ PB: gelieve het nummer van deze verordening in te vullen (2021/0106(COD)).

Artikel 109

Wijziging van Verordening (EU) 2019/2144

Aan artikel 11 van Verordening (EU) 2019/2144 wordt het volgende lid toegevoegd:

- “3. Bij het vaststellen van de uitvoeringshandelingen krachtens lid 2 betreffende artificiële-intelligentiesystemen die veiligheidscomponenten zijn in de zin van Verordening (EU) 2024/... van het Europees Parlement en de Raad^{*,+}, worden de eisen van hoofdstuk III, afdeling 2, van die verordening in aanmerking genomen.

* Verordening (EU) 2024/... van het Europees Parlement en de Raad van ... tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...).”.

⁺ PB: gelieve in de tekst het nummer van deze verordening (2021/0106(COD)) in te vullen en de voetnoot te vervolledigen.

Artikel 110

Wijziging van Richtlijn (EU) 2020/1828

In bijlage I bij Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad⁵⁸ wordt het volgende punt toegevoegd:

“68) Verordening (EU) 2024/...⁺ van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144 en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (verordening artificiële intelligentie) (PB L, ..., ELI: ...)”.

Artikel 111

Reeds in de handel gebrachte of in gebruik gestelde AI-systemen

1. Onverminderd de toepassing van artikel 5 als bedoeld in artikel 113, lid 3, punt a), worden AI-systemen die componenten zijn van de bij de in bijlage X vermelde rechtshandelingen opgezette grootschalige IT-systemen die vóór ... [36 maanden na de datum van inwerkingtreding van deze verordening] in de handel zijn gebracht of in gebruik zijn gesteld, uiterlijk op 31 december 2030 in overeenstemming met deze verordening gebracht.

⁵⁸ Richtlijn (EU) 2020/1828 van het Europees Parlement en de Raad van 25 november 2020 betreffende representatieve vorderingen ter bescherming van de collectieve belangen van consumenten en tot intrekking van Richtlijn 2009/22/EG (PB L 409 van 4.12.2020, blz. 1).
⁺ PB: gelieve het nummer van deze verordening in te vullen (2021/0106(COD)).

De in deze verordening vastgelegde eisen worden in aanmerking genomen bij de evaluatie van elk volgens de in bijlage X vermelde rechtshandelingen opgezet grootschalig IT-systeem die moet worden uitgevoerd zoals bepaald in die rechtshandelingen en wanneer die rechtshandelingen worden vervangen of gewijzigd.

2. Onverminderd de toepassing van artikel 5 als bedoeld in artikel 113, lid 3, punt a), is deze verordening alleen van toepassing op operatoren van AI-systemen met een hoog risico, met uitzondering van de in lid 1 van dit artikel bedoelde systemen, die vóór ... [24 maanden na de datum van inwerkingtreding van deze verordening] in de handel zijn gebracht of in gebruik zijn gesteld indien die systemen vanaf die datum aanzienlijke wijzigingen in hun ontwerp ondergaan. In ieder geval ondernemen de aanbieders en gebruiksverantwoordelijken van AI-systemen met een hoog risico die bedoeld zijn om door overheidsinstanties te worden gebruikt, de nodige stappen om uiterlijk op ... [zes jaar na de datum van inwerkingtreding van deze verordening] aan de eisen en verplichtingen van deze verordening te voldoen.
3. Aanbieders van AI-modellen voor algemene doeleinden die vóór ... [12 maanden na de datum van inwerkingtreding van deze verordening] in de handel zijn gebracht, ondernemen de nodige stappen om uiterlijk op ... [36 maanden na de datum van inwerkingtreding van deze verordening] aan de verplichtingen van deze verordening te voldoen.

Artikel 112
Evaluatie en toetsing

1. De Commissie beoordeelt vanaf de inwerkingtreding van deze verordening en tot het einde van de in artikel 97 vermelde periode van de bevoegdheidsdelegatie eenmaal per jaar of de lijst van bijlage III en de lijst van de verboden AI-praktijken in artikel 5 moeten worden gewijzigd. De Commissie deelt de bevindingen van die beoordeling mee aan het Europees Parlement en de Raad.
2. Uiterlijk op ... [vier jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de vier jaar verricht de Commissie een evaluatie en brengt zij verslag uit bij het Europees Parlement en de Raad over het volgende:
 - a) de noodzaak om bestaande gebiedsrubrieken uit te breiden of nieuwe gebiedsrubrieken toe te voegen aan bijlage III;
 - b) wijzigingen van de lijst van AI-systemen die aanvullende transparantiemaatregelen vereisen krachtens artikel 50;
 - c) wijzigingen ter verbetering van de doeltreffendheid van het toezicht- en governancesysteem.

3. Uiterlijk op ... [vijf jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de vier jaar dient de Commissie bij het Europees Parlement en de Raad een verslag in over de evaluatie en de toetsing van deze verordening. Het verslag bevat een beoordeling van de structuur van de handhaving en de eventuele noodzaak van een agentschap van de Unie om vastgestelde tekortkomingen op te lossen. Op basis van de bevindingen gaat dat verslag indien passend vergezeld van een voorstel tot wijziging van deze verordening. De verslagen worden openbaar gemaakt.
4. In de in lid 2 bedoelde verslagen wordt specifieke aandacht besteed aan het volgende:
- a) de status van de financiële, technische en personele middelen van de nationale bevoegde autoriteiten teneinde de hun krachtens deze verordening toegewezen taken doeltreffend uit te voeren;
 - b) de stand van zaken wat betreft sancties, met name administratieve geldboeten als bedoeld in artikel 99, lid 1, die door lidstaten zijn toegepast wegens inbreuken op deze verordening;
 - c) ter ondersteuning van deze verordening aangenomen geharmoniseerde normen en ontwikkelde gemeenschappelijke specificaties;
 - d) het aantal ondernemingen, met daarbij ook het aantal kmo's, dat nadat deze verordening van toepassing is geworden tot de markt toetreedt.

5. Uiterlijk op ... [vier jaar na de inwerkingtreding van deze verordening] evalueert de Commissie de werking van het AI-bureau, de vraag of het Bureau voldoende bevoegdheden heeft gekregen om zijn taken uit te voeren en of het voor de correcte uitvoering en handhaving van deze verordening relevant en noodzakelijk zou zijn om het AI-bureau en zijn handhavingsbevoegdheden op te schalen en zijn middelen uit te breiden. De Commissie dient dit evaluatieverslag in bij het Europees Parlement en bij de Raad.
6. Uiterlijk op ... [vier jaar na de datum van inwerkingtreding van deze verordening] en vervolgens om de vier jaar dient de Commissie een verslag in met een evaluatie van de vooruitgang bij de ontwikkeling van normalisatieproducten met betrekking tot de energie-efficiënte ontwikkeling van AI-modellen voor algemene doeleinden, en beoordeelt zij of verdere al dan niet bindende maatregelen of acties nodig zijn. Dit verslag wordt toegezonden aan het Europees Parlement en de Raad en openbaar gemaakt.
7. Uiterlijk op ... [vier jaar na de inwerkingtreding van deze verordening] en vervolgens om de drie jaar evalueert de Commissie de impact en de doeltreffendheid van vrijwillige gedragscodes om de toepassing van de eisen van hoofdstuk III, afdeling 2, voor AI-systemen die geen AI-systemen met een hoog risico zijn en eventuele andere aanvullende eisen voor AI-systemen die geen AI-systemen met een hoog risico zijn te bevorderen, ook wat betreft milieuduurzaamheid.
8. Voor de toepassing van de leden 1 tot en met 7 verstrekken de AI-board, de lidstaten en nationale bevoegde autoriteiten onverwijld informatie aan de Commissie op haar verzoek.

9. Bij de uitvoering van de in de leden 1 tot en met 7 vermelde evaluaties en toetsingen neemt de Commissie de standpunten en bevindingen van de AI-board, het Europees Parlement, de Raad en van andere relevante instanties of bronnen in aanmerking.
10. Indien nodig dient de Commissie passende voorstellen in teneinde deze verordening te wijzigen, met name rekening houdend met ontwikkelingen in de technologie, het effect van AI-systemen op gezondheid en veiligheid, en op de grondrechten, en de voortgang in de informatiemaatschappij.
11. Om de evaluaties en toetsingen als bedoeld in de leden 1 tot en met 7 van dit artikel uit te voeren, ontwikkelt het AI-bureau een objectieve en participatieve methodologie voor de evaluatie van de risiconiveaus, op basis van de in de desbetreffende artikelen beschreven criteria en opname van nieuwe systemen in:
- a) de lijst in bijlage III, waaronder de uitbreiding van bestaande gebiedsrubrieken of de toevoeging van nieuwe rubrieken in die bijlage;
 - b) de lijst van verboden praktijken als vastgelegd in artikel 5; en
 - c) de lijst van AI-systemen die aanvullende transparantieverplichtingen met zich meebrengen op grond van artikel 50.
12. Elke wijziging van deze verordening op grond van lid 10, of relevante gedelegeerde handelingen of uitvoeringshandelingen, die betrekking heeft op sectorale harmonisatiewetgeving van de Unie zoals vermeld in bijlage I, afdeling B, wordt rekening gehouden met de regelgevingsspecificaties van elke sector, met de bestaande mechanismen voor governance, conformiteitsbeoordeling en handhaving en met de autoriteiten die daarin zijn vastgesteld.

13. Uiterlijk op ... [zeven jaar na de inwerkingtreding van deze verordening] voert de Commissie een beoordeling uit van de handhaving van deze verordening en brengt hierover verslag uit aan het Europees Parlement, de Raad en het Europees Economisch en Sociaal Comité, waarbij de eerste jaren van toepassing van deze verordening worden meegenomen. Op basis van de bevindingen gaat dit verslag, indien van toepassing, vergezeld van een voorstel tot wijziging van deze verordening met betrekking tot de handhavingsstructuur en de behoefte aan een agentschap van de Unie om eventueel vastgestelde tekortkomingen op te lossen.

Artikel 113

Inwerkingtreding en toepassing

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Zij is van toepassing met ingang van ... [24 maanden na de datum van de inwerkingtreding van deze verordening].

Evenwel zijn:

- a) de hoofdstukken I en II van toepassing met ingang van ... [zes maanden na de datum van de inwerkingtreding van deze verordening];
- b) hoofdstuk III, afdeling 4, hoofdstuk V, hoofdstuk VII en hoofdstuk XII en artikel 78 van toepassing met ingang van ... [12 maanden na de datum van inwerkingtreding van deze verordening], met uitzondering van artikel 101;

- c) artikel 6, lid 1, en de overeenkomstige verplichtingen van deze verordening van toepassing met ingang van ... [36 maanden na de datum van inwerkingtreding van deze verordening].

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel,

Voor het Europees Parlement

De voorzitter

Voor de Raad

De voorzitter

BIJLAGE I

Lijst van harmonisatiewetgeving van de Unie

Afdeling A – Lijst van harmonisatiewetgeving van de Unie op basis van het nieuwe wetgevingskader

1. Richtlijn 2006/42/EG van het Europees Parlement en de Raad van 17 mei 2006 betreffende machines en tot wijziging van Richtlijn 95/16/EG (PB L 157 van 9.6.2006, blz. 24);
2. Richtlijn 2009/48/EG van het Europees Parlement en de Raad van 18 juni 2009 betreffende de veiligheid van speelgoed (PB L 170 van 30.6.2009, blz. 1);
3. Richtlijn 2013/53/EU van het Europees Parlement en de Raad van 20 november 2013 betreffende pleziervaartuigen en waterscooters en tot intrekking van Richtlijn 94/25/EG (PB L 354 van 28.12.2013, blz. 90);
4. Richtlijn 2014/33/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake liften en veiligheidscomponenten voor liften (PB L 96 van 29.3.2014, blz. 251);
5. Richtlijn 2014/34/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake apparaten en beveiligingssystemen bedoeld voor gebruik op plaatsen waar ontploffingsgevaar kan heersen (PB L 96 van 29.3.2014, blz. 309);

6. Richtlijn 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PB L 153 van 22.5.2014, blz. 62);
7. Richtlijn 2014/68/EU van het Europees Parlement en de Raad van 15 mei 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van drukapparatuur (PB L 189 van 27.6.2014, blz. 164);
8. Verordening (EU) 2016/424 van het Europees Parlement en de Raad van 9 maart 2016 betreffende kabelbaaninstallaties en tot intrekking van Richtlijn 2000/9/EG (PB L 81 van 31.3.2016, blz. 1);
9. Verordening (EU) 2016/425 van het Europees Parlement en de Raad van 9 maart 2016 betreffende persoonlijke beschermingsmiddelen en tot intrekking van Richtlijn 89/686/EEG van de Raad (PB L 81 van 31.3.2016, blz. 51);
10. Verordening (EU) 2016/426 van het Europees Parlement en de Raad van 9 maart 2016 betreffende gasverbrandingstoestellen en tot intrekking van Richtlijn 2009/142/EG (PB L 81 van 31.3.2016, blz. 99);
11. Verordening (EU) 2017/745 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen, tot wijziging van Richtlijn 2001/83/EG, Verordening (EG) nr. 178/2002 en Verordening (EG) nr. 1223/2009, en tot intrekking van Richtlijnen 90/385/EEG en 93/42/EEG van de Raad (PB L 117 van 5.5.2017, blz. 1);

12. Verordening (EU) 2017/746 van het Europees Parlement en de Raad van 5 april 2017 betreffende medische hulpmiddelen voor in-vitrodiagnostiek en tot intrekking van Richtlijn 98/79/EG en Besluit 2010/227/EU van de Commissie (PB L 117 van 5.5.2017, blz. 176).

Afdeling B – Lijst van andere harmonisatiewetgeving van de Unie

13. Verordening (EG) nr. 300/2008 van het Europees Parlement en de Raad van 11 maart 2008 inzake gemeenschappelijke regels op het gebied van de beveiliging van de burgerluchtvaart en tot intrekking van Verordening (EG) nr. 2320/2002 (PB L 97 van 9.4.2008, blz. 72);
14. Verordening (EU) nr. 168/2013 van het Europees Parlement en de Raad van 15 januari 2013 betreffende de goedkeuring van en het markttoezicht op twee- of driewielige voertuigen en vierwielers (PB L 60 van 2.3.2013, blz. 52);
15. Verordening (EU) nr. 167/2013 van het Europees Parlement en de Raad van 5 februari 2013 inzake de goedkeuring van en het markttoezicht op landbouw- en bosbouwvoertuigen (PB L 60 van 2.3.2013, blz. 1);
16. Richtlijn 2014/90/EU van het Europees Parlement en de Raad van 23 juli 2014 inzake uitrusting van zeeschepen en tot intrekking van Richtlijn 96/98/EG van de Raad (PB L 257 van 28.8.2014, blz. 146);
17. Richtlijn (EU) 2016/797 van het Europees Parlement en de Raad van 11 mei 2016 betreffende de interoperabiliteit van het spoorwegsysteem in de Europese Unie (PB L 138 van 26.5.2016, blz. 44);

18. Verordening (EU) 2018/858 van het Europees Parlement en de Raad van 30 mei 2018 betreffende de goedkeuring van en het markttoezicht op motorvoertuigen en aanhangwagens daarvan en systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd, tot wijziging van Verordeningen (EG) nr. 715/2007 en (EG) nr. 595/2009 en tot intrekking van Richtlijn 2007/46/EG (PB L 151 van 14.6.2018, blz. 1);
19. Verordening (EU) 2019/2144 van het Europees Parlement en de Raad van 27 november 2019 betreffende de voorschriften voor de typegoedkeuring van motorvoertuigen en aanhangwagens daarvan en van systemen, onderdelen en technische eenheden die voor dergelijke voertuigen zijn bestemd wat de algemene veiligheid ervan en de bescherming van de inzittenden van voertuigen en kwetsbare weggebruikers betreft, tot wijziging van Verordening (EU) 2018/858 van het Europees Parlement en de Raad en tot intrekking van de Verordeningen (EG) nr. 78/2009, (EG) nr. 79/2009 en (EG) nr. 661/2009 van het Europees Parlement en de Raad en de Verordeningen (EG) nr. 631/2009, (EU) nr. 406/2010, (EU) nr. 672/2010, (EU) nr. 1003/2010, (EU) nr. 1005/2010, (EU) nr. 1008/2010, (EU) nr. 1009/2010, (EU) nr. 19/2011, (EU) nr. 109/2011, (EU) nr. 458/2011, (EU) nr. 65/2012, (EU) nr. 130/2012, (EU) nr. 347/2012, (EU) nr. 351/2012, (EU) nr. 1230/2012 en (EU) 2015/166 van de Commissie (PB L 325 van 16.12.2019, blz. 1);

20. Verordening (EU) 2018/1139 van het Europees Parlement en de Raad van 4 juli 2018 inzake gemeenschappelijke regels op het gebied van burgerluchtvaart en tot oprichting van een Agentschap van de Europese Unie voor de veiligheid van de luchtvaart, en tot wijziging van de Verordeningen (EG) nr. 2111/2005, (EG) nr. 1008/2008, (EU) nr. 996/2010, (EU) nr. 376/2014 en de Richtlijnen 2014/30/EU en 2014/53/EU van het Europees Parlement en de Raad, en tot intrekking van de Verordeningen (EG) nr. 552/2004 en (EG) nr. 216/2008 van het Europees Parlement en de Raad en Verordening (EEG) nr. 3922/91 van de Raad (PB L 212 van 22.8.2018, blz. 1), voor zover het gaat om het ontwerp, de productie en het in de handel brengen van luchtvaartuigen als bedoeld in artikel 2, lid 1, punten a) en b), wat betreft onbemande luchtvaartuigen, en hun motoren, propellers, onderdelen en apparatuur om het luchtvaartuig op afstand te besturen.
-

BIJLAGE II

Lijst van in artikel 5, lid 1, eerste alinea, punt h), iii), bedoelde strafbare feiten

Strafbare feiten als bedoeld in artikel 5, lid 1, eerste alinea, punt e), onder iii):

- terrorisme,
- mensenhandel,
- seksuele uitbuiting van kinderen en kinderpornografie,
- illegale handel in verdovende middelen of psychotrope stoffen,
- illegale handel in wapens, munitie of explosieven,
- moord, zware mishandeling,
- illegale handel in menselijke organen of weefsels,
- illegale handel in nucleaire of radioactieve stoffen,
- ontvoering, wederrechtelijke vrijheidsberoving of gijzeling,
- misdrijven die onder de rechtsmacht van het Internationaal Strafhof vallen,
- kaping van vliegtuigen of schepen,

- verkrachting,
 - milieucriminaliteit,
 - georganiseerde of gewapende diefstal,
 - sabotage,
 - deelneming aan een criminele organisatie die betrokken is bij een of meer van de hierboven genoemde strafbare feiten.
-

BIJLAGE III

In artikel 6, lid 2, bedoelde AI-systemen met een hoog risico

AI-systemen met een hoog risico op grond van artikel 6, lid 2, zijn de vermelde AI-systemen op de volgende gebieden:

1. Biometrie, voor zover het gebruik ervan is toegestaan op grond van het toepasselijke Unierecht of nationale recht:

a) Systemen voor biometrische identificatie op afstand.

Dit geldt niet voor AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie met als enig doel te bevestigen dat een specifieke natuurlijke persoon de persoon is die hij of zij beweert te zijn;

b) AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische categorisering op basis van gevoelige of beschermde eigenschappen of kenmerken, of op basis van wat uit die eigenschappen of kenmerken wordt afgeleid;

c) AI-systemen die bedoeld zijn om te worden gebruikt voor emotieherkenning.

2. Kritieke infrastructuur: AI-systemen die bedoeld zijn om te worden gebruikt als veiligheidscomponent bij het beheer of de exploitatie van kritieke digitale infrastructuur, wegverkeer of bij de levering van water, gas, verwarming en elektriciteit.

3. Onderwijs en beroepsopleiding:

- a) AI-systemen die bedoeld zijn om te worden gebruikt voor het bepalen van toegang of toelating tot of het toewijzen van natuurlijke personen aan instellingen voor onderwijs en beroepsonderwijs op alle niveaus;
- b) AI-systemen die bedoeld zijn om te worden gebruikt voor het evalueren van leerresultaten, ook wanneer die resultaten worden gebruikt voor het sturen van het leerproces van natuurlijke personen in instellingen voor onderwijs en beroepsonderwijs op alle niveaus;
- c) AI-systemen die bedoeld zijn om te worden gebruikt voor het beoordelen van het passende onderwijsniveau dat een persoon zal ontvangen of waartoe hij toegang zal hebben, in het kader van of binnen instellingen voor onderwijs en beroepsonderwijs op alle niveaus;
- d) AI-systemen die bedoeld zijn om te worden gebruikt voor het monitoren en detecteren van ongeoorloofd gedrag van studenten tijdens toetsen in de context van of binnen instellingen voor onderwijs en beroepsonderwijs op alle niveaus.

4. Werkgelegenheid, personeelsbeheer en toegang tot zelfstandige arbeid:

- a) AI-systemen die bedoeld zijn om te worden gebruikt voor het werven of selecteren van natuurlijke personen, met name voor het plaatsen van gerichte vacatures, het analyseren en filteren van sollicitaties, en het beoordelen van kandidaten;

- b) AI-systemen die bedoeld zijn om te worden gebruikt voor het nemen van besluiten die van invloed zijn op de voorwaarden van arbeidsgerelateerde betrekkingen, de bevordering of beëindiging van arbeidsgerelateerde contractuele betrekkingen, voor het toewijzen van taken op basis van individueel gedrag of persoonlijke eigenschappen of kenmerken, of voor het monitoren en evalueren van prestaties en gedrag van personen in dergelijke betrekkingen.

5. Toegang tot en gebruik van essentiële particuliere en publieke diensten en uitkeringen:

- a) AI-systemen die bedoeld zijn om door of namens overheidsinstanties te worden gebruikt om te beoordelen of natuurlijke personen in aanmerking komen voor essentiële overheidsuitkeringen en -diensten, waaronder gezondheidsdiensten, of om dergelijke uitkeringen en diensten te verlenen, te beperken, in te trekken of terug te vorderen;
- b) AI-systemen die bedoeld zijn om te worden gebruikt voor het beoordelen van de kredietwaardigheid van natuurlijke personen of voor het vaststellen van hun kredietscore, met uitzondering van AI-systemen die gebruikt worden om financiële fraude op te sporen;
- c) AI-systemen die bedoeld zijn om te worden gebruikt voor risicobeoordeling en prijsstelling met betrekking tot natuurlijke personen in het geval van levens- en ziektekostenverzekeringen;
- d) AI-systemen die bedoeld zijn om noodoproepen van natuurlijke personen te evalueren en te classificeren of om te worden gebruikt voor het inzetten of het bepalen van prioriteiten voor de inzet van hulpdiensten, onder meer van politie, brandweer en ambulance, alsook van systemen voor de triage van patiënten die dringend medische zorg behoeven.

6. Rechtshandhaving, voor zover het gebruik ervan is toegestaan op grond van het toepasselijke Unierecht of nationale recht:
- a) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties, of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties of namens hen, te worden gebruikt om het risico te beoordelen dat een natuurlijke persoon het slachtoffer wordt van strafbare feiten;
 - b) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt als leugendetector of soortgelijke instrumenten;
 - c) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt om de betrouwbaarheid van bewijsmateriaal tijdens het onderzoek naar of de vervolging van strafbare feiten te beoordelen;
 - d) AI-systemen die bedoeld zijn om door of namens rechtshandhavingsinstanties of door instellingen, organen of instanties van de Unie ter ondersteuning van rechtshandhavingsinstanties te worden gebruikt om te beoordelen hoe groot het risico is dat een natuurlijke persoon (opnieuw) een strafbaar feit zal plegen, niet uitsluitend op basis van profilering van natuurlijke personen als bedoeld in artikel 3, punt 4, van Richtlijn (EU) 2016/680, of om persoonlijkheidskenmerken en eigenschappen of eerder crimineel gedrag van natuurlijke personen of groepen te beoordelen;

- e) AI-systemen die bedoeld zijn om door of namens rechtshandavingsinstanties of door instellingen, organen en instanties van de Unie ter ondersteuning van rechtshandavingsinstanties te worden gebruikt om natuurlijke personen te profileren als bedoeld in artikel 3, punt 4, van Richtlijn (EU) 2016/680, tijdens het opsporen, onderzoeken of vervolgen van strafbare feiten.

7. Migratie-, asiel- en grenstoezichtsbeheer, voor zover het gebruik ervan is toegestaan op grond van het toepasselijke Unierecht of nationale recht:

- a) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties of door instellingen, organen of instanties van de Unie te worden gebruikt als leugendetector of soortgelijke hulpmiddelen;
- b) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties of door instellingen, organen of instanties van de Unie te worden gebruikt om risico's te beoordelen, waaronder een veiligheidsrisico, een risico op illegale migratie of een gezondheidsrisico, uitgaat van een natuurlijke persoon die voornemens is het grondgebied van een lidstaat te betreden of dat heeft gedaan;
- c) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties of door instellingen, organen of instanties van de Unie te worden gebruikt om bevoegde overheidsinstanties bij te staan bij de behandeling van aanvragen voor asiel, visa of verblijfsvergunningen en bij de behandeling van aanverwante klachten in verband met het al dan niet in aanmerking komen van de natuurlijke personen die een aanvraag voor een status indienen, met inbegrip van hieraan gerelateerde beoordelingen van de betrouwbaarheid van bewijsmateriaal;

- d) AI-systemen die bedoeld zijn om door of namens bevoegde overheidsinstanties, of door instellingen, organen of instanties van de Unie, te worden gebruikt in het kader van migratie-, asiel- of grenstoezichtsbeheer, met het oog op het opsporen, herkennen of identificeren van natuurlijke personen, met uitzondering van de verificatie van reisdocumenten.

8. Rechtsbedeling en democratische processen:

- a) AI-systemen die bedoeld zijn om door of namens een gerechtelijke instantie te worden gebruikt om een gerechtelijke instantie te ondersteunen bij het onderzoeken en uitleggen van feiten of de wet en bij de toepassing van het recht op een concrete reeks feiten of om te worden gebruikt op soortgelijke wijze in het kader van alternatieve geschillenbeslechting;
- b) AI-systemen die bedoeld zijn om te worden gebruikt voor het beïnvloeden van de uitslag van een verkiezing of referendum of van het stemgedrag van natuurlijke personen bij de uitoefening van hun stemrecht bij verkiezingen of referenda. Dit geldt niet voor AI-systemen aan de output waarvan natuurlijke personen niet rechtstreeks worden blootgesteld, zoals instrumenten die worden gebruikt om politieke campagnes te organiseren, te optimaliseren of te structureren vanuit administratief of logistiek oogpunt.

BIJLAGE IV

Technische documentatie als bedoeld in artikel 11, lid 1

De technische documentatie als bedoeld in artikel 11, lid 1, bevat ten minste de volgende informatie, zoals van toepassing op het betreffende AI-systeem:

1. Een algemene beschrijving van het AI-systeem, met daarin:
 - a) het beoogde doel, de naam van de aanbieder en de versie van het systeem, waarbij het verband met eerdere versies duidelijk gemaakt wordt;
 - b) hoe het AI-systeem interageert of kan worden gebruikt om te interageren met hardware of software, ook met andere AI-systemen die geen deel uitmaken van het AI-systeem zelf, indien van toepassing;
 - c) de versies van de betreffende software of firmware en eventuele eisen met betrekking tot versie-updates;
 - d) de beschrijving van alle vormen waarin het AI-systeem in de handel wordt gebracht of in gebruik wordt gesteld, zoals in hardware ingebedde softwarepakketten, downloads of API's;
 - e) de beschrijving van de hardware waarop het AI-systeem moet worden uitgevoerd;
 - f) indien het AI-systeem een component vormt van producten, foto's of illustraties: de externe kenmerken, markeringen en interne lay-out van die producten;

- g) een basisbeschrijving van de gebruikersinterface die aan de gebruiksverantwoordelijke wordt verstrekt;
 - h) gebruiksinstructies voor de gebruiksverantwoordelijke en een basisbeschrijving van de gebruikersinterface die aan de gebruiksverantwoordelijke wordt verstrekt, indien van toepassing.
2. Een gedetailleerde beschrijving van de elementen van het AI-systeem en van het proces voor de ontwikkeling ervan, waaronder:
- a) de uitgevoerde methoden en stappen voor de ontwikkeling van het AI-systeem, met inbegrip van, indien relevant, het gebruik van door derden geleverde vooraf getrainde systemen of hulpmiddelen en hoe die zijn gebruikt, geïntegreerd of aangepast door de aanbieder;
 - b) de ontwerpspecificaties van het systeem, met name de algemene logica van het AI-systeem en van de algoritmen; de belangrijkste ontwerpkeuzen, waaronder de motivering en de gedane aannamen, ook met betrekking tot personen of groepen personen ten aanzien van wie het systeem bedoeld is om te worden gebruikt; de belangrijkste classificatiekeuzen; voor welke optimalisatie het systeem is ontworpen en de relevantie van de verschillende parameters; de beschrijving van de verwachte output en outputkwaliteit van het systeem; de beslissingen ten aanzien van eventuele afwegingen met betrekking tot technische oplossingen die zijn vastgesteld om te voldoen aan de eisen van hoofdstuk III, afdeling 2;
 - c) de beschrijving van de systeemarchitectuur met een toelichting bij hoe softwarecomponenten op elkaar voortbouwen of elkaar informatie aanleveren en hoe de integratie in de algemene verwerking plaatsvindt; de rekenhulpmiddelen die zijn gebruikt voor het ontwikkelen, trainen, testen en valideren van het AI-systeem;

- d) indien relevant, de datavereisten voor de informatiebladen waarop de trainingsmethoden en -technieken zijn beschreven en de gebruikte reeksen trainingsdata, met inbegrip van een algemene beschrijving van deze datasets en informatie over de herkomst, reikwijdte en belangrijkste kenmerken ervan; hoe de data zijn verkregen en geselecteerd; labelingprocedures (bv. voor gecontroleerd leren), methoden voor dataopschoning (bv. opsporing van uitschieters);
- e) een beoordeling van de in overeenstemming met artikel 14 benodigde maatregelen op het gebied van menselijk toezicht, waaronder een beoordeling van de benodigde technische maatregelen voor de vereenvoudiging van de interpretatie van de output van AI-systemen door gebruiksverantwoordelijken, in overeenstemming met artikel 13, lid 3, punt d);
- f) indien van toepassing, een gedetailleerde beschrijving van vooraf bepaalde wijzigingen in het AI-systeem en de prestaties ervan, samen met alle relevante informatie die verband houdt met de technische oplossingen die zijn ingevoerd om de voortdurende naleving door het AI-systeem van de relevante eisen van hoofdstuk III, afdeling 2, te waarborgen;
- g) de gebruikte validatie- en testprocedures, waaronder informatie over de gebruikte validatie- en testdata en de belangrijkste kenmerken ervan; de statistieken die worden gebruikt voor het meten van de nauwkeurigheid, robuustheid, en naleving van andere relevante eisen van hoofdstuk III, afdeling 2, evenals mogelijk discriminerende gevolgen; logbestanden over en alle verslagen van tests die zijn gedateerd en ondertekend door de verantwoordelijken, waaronder met betrekking tot vooraf vastgestelde wijzigingen als bedoeld in punt f);
- h) gehanteerde cyberbeveiligingsmaatregelen.

3. Gedetailleerde informatie over de monitoring, werking en controle van het AI-systeem, meer bepaald met betrekking tot: de mogelijkheden en beperkingen op het gebied van de prestaties van het systeem, waaronder de verschillende maten van nauwkeurigheid voor specifieke personen of groepen personen waarvoor het systeem bedoeld is om te worden gebruikt en het totale verwachte nauwkeurngheidsniveau in verhouding tot het beoogde doel; de voorzienbare onbedoelde resultaten en risicobronnen voor de gezondheid en veiligheid, de grondrechten en discriminatie gelet op het beoogde doel van het AI-systeem; de in overeenstemming met artikel 14 benodigde maatregelen voor menselijk toezicht, met inbegrip van de technische maatregelen die zijn getroffen om de interpretatie van de output van AI-systemen door gebruiksverantwoordelijken te vergemakkelijken; specificaties over inputdata, indien van toepassing.
4. Een beschrijving van de geschiktheid van de prestatiestatistieken voor het specifieke AI-systeem.
5. Een gedetailleerde beschrijving van het systeem voor risicobeheer overeenkomstig artikel 9.
6. Een beschrijving van de relevante wijzigingen die door de aanbieder tijdens de levensduur van het systeem erin worden aangebracht.
7. Een lijst van de geharmoniseerde normen die volledig of gedeeltelijk worden toegepast en waarvan de referenties zijn gepubliceerd in het *Publicatieblad van de Europese Unie*. Indien dergelijke geharmoniseerde normen niet zijn toegepast, een gedetailleerde beschrijving van de vastgestelde oplossingen om te voldoen aan de eisen van hoofdstuk III, afdeling 2, met inbegrip van een lijst van andere toegepaste relevante normen en technische specificaties.
8. Een exemplaar van de in artikel 47 bedoelde EU-conformiteitsverklaring.
9. Een gedetailleerde beschrijving van het ingevoerde systeem voor de evaluatie van de prestaties van het AI-systeem nadat het in de handel is gebracht, in overeenstemming met artikel 72, met inbegrip van het in artikel 72, lid 3, bedoelde plan voor monitoring na het in de handel brengen.

BIJLAGE V

EU-conformiteitsverklaring

De in artikel 47 bedoelde EU-conformiteitsverklaring bevat de volgende informatie:

1. de naam en het type van het AI-systeem, evenals eventuele aanvullende ondubbelzinnige verwijzingen waarmee het AI-systeem kan worden geïdentificeerd en getraceerd;
2. de naam en het adres van de aanbieder en, indien van toepassing, zijn gemachtigde;
3. een vermelding dat de in artikel 47 bedoelde EU-conformiteitsverklaring wordt verstrekt onder de uitsluitende verantwoordelijkheid van de aanbieder;
4. een vermelding dat het AI-systeem in overeenstemming is met deze verordening en, in voorkomend geval, met eventuele andere desbetreffende Uniewetgeving die voorziet in de afgifte van de in artikel 47 bedoelde EU-conformiteitsverklaring;
5. indien een AI-systeem de verwerking van persoonsgegevens met zich meebrengt, een verklaring dat dat AI-systeem voldoet aan de Verordeningen (EU) 2016/679 en (EU) 2018/1725 en Richtlijn (EU) 2016/680;
6. de vermelding van eventuele toegepaste relevante geharmoniseerde normen of van andere gemeenschappelijke specificaties waarop de conformiteitsverklaring betrekking heeft;

7. indien van toepassing, de naam en het identificatienummer van de aangemelde instantie, een beschrijving van de uitgevoerde conformiteitsbeoordelingsprocedure en identificatie van het afgegeven certificaat;
8. de plaats en de datum van afgifte van de verklaring, de naam en de functie van de persoon die de verklaring heeft ondertekend alsmede een vermelding van de persoon voor en namens wie die persoon ondertekent, een handtekening.

BIJLAGE VI

Conformiteitsbeoordelingsprocedure op basis van interne controle

1. De conformiteitsbeoordelingsprocedure op basis van interne controle is de conformiteitsbeoordelingsprocedure op basis van de punten 2, 3 en 4.
 2. De aanbieder verifieert dat het ingevoerde kwaliteitsbeheersysteem voldoet aan de eisen van artikel 17.
 3. De aanbieder beoordeelt de in de technische documentatie opgenomen informatie om te beoordelen of het AI-systeem voldoet aan de relevante essentiële eisen van hoofdstuk III, afdeling 2.
 4. De aanbieder verifieert eveneens of het ontwerp- en ontwikkelingsproces van het AI-systeem en de in artikel 72 bedoelde monitoring na het in de handel brengen overeenkomt met de technische documentatie.
-

BIJLAGE VII

Conformiteit op basis van een beoordeling van het kwaliteitsbeheersysteem
en een beoordeling van de technische documentatie

1. Inleiding

De conformiteit op basis van een beoordeling van het kwaliteitsbeheersysteem en een beoordeling van de technische documentatie is de conformiteitsbeoordelingsprocedure op basis van de punten 2 tot en met 5.

2. Overzicht

Het op grond van artikel 17 goedgekeurde kwaliteitsbeheersysteem voor het ontwerp, de ontwikkeling en het testen van AI-systemen wordt beoordeeld in overeenstemming met punt 3 en is onderworpen aan het in punt 5 bedoelde toezicht. De technische documentatie van het AI-systeem wordt beoordeeld in overeenstemming met punt 4.

3. Systeem voor kwaliteitsbeheer

3.1. De aanvraag van de aanbieder bevat onder meer:

- a) de naam en het adres van de aanbieder en, indien de aanvraag wordt ingediend door een gemachtigde, ook diens naam en adres;
- b) de lijst met AI-systemen die vallen onder hetzelfde kwaliteitsbeheersysteem;
- c) de technische documentatie voor elk AI-systeem dat valt onder hetzelfde kwaliteitsbeheersysteem;

- d) de documentatie betreffende het kwaliteitsbeheersysteem, dat alle in artikel 17 vermelde aspecten beslaat;
- e) een beschrijving van de ingestelde procedures om te zorgen dat het kwaliteitsbeheersysteem adequaat en doeltreffend blijft;
- f) een schriftelijke verklaring dat er geen gelijklopende aanvraag bij een andere aangemelde instantie is ingediend.

3.2. Het kwaliteitsbeheersysteem wordt beoordeeld door de aangemelde instantie, die bepaalt of wordt voldaan aan de in artikel 17 bedoelde eisen.

Het besluit wordt meegedeeld aan de aanbieder of diens gemachtigde.

In deze kennisgeving zijn de conclusies van de beoordeling van het kwaliteitsbeheersysteem opgenomen, evenals de met redenen omklede beoordelingsbeslissing.

3.3. Het goedgekeurde kwaliteitsbeheersysteem wordt zodanig uitgevoerd en onderhouden door de aanbieder dat het toereikend en efficiënt blijft.

3.4. Voorgenomen wijzigingen in het goedgekeurde kwaliteitsbeheersysteem of de lijst met AI-systemen waarop het beheersysteem van toepassing is, worden door de aanbieder meegedeeld aan de aangemelde instantie.

De voorgestelde wijzigingen worden beoordeeld door de aangemelde instantie, die beslist of het gewijzigde kwaliteitsbeheersysteem blijft voldoen aan de in punt 3.2 bedoelde eisen dan wel of een nieuwe beoordeling noodzakelijk is.

De aangemelde instantie stelt de aanbieder in kennis van haar beslissing. In deze kennisgeving zijn de conclusies van de beoordeling van de wijzigingen opgenomen, evenals de met redenen omklede beoordelingsbeslissing.

4. Controle van de technische documentatie.
 - 4.1. In aanvulling op de in punt 3 bedoelde aanvraag, wordt een aanvraag bij een aangemelde instantie naar keuze ingediend door de aanbieder voor de beoordeling van de technische documentatie die betrekking heeft op het AI-systeem dat de aanbieder voornemens is in de handel te brengen of in gebruik te stellen en waarop het in punt 3 bedoelde kwaliteitsbeheersysteem van toepassing is.
 - 4.2. De aanvraag omvat:
 - a) de naam en het adres van de aanbieder;
 - b) een schriftelijke verklaring dat er geen gelijklopende aanvraag bij een andere aangemelde instantie is ingediend;
 - c) de in bijlage IV bedoelde technische documentatie.
 - 4.3. De technische documentatie wordt beoordeeld door de aangemelde instantie. Indien relevant en beperkt tot wat nodig is om haar taken uit te voeren, wordt aan de aangemelde instantie volledige toegang verleend tot de gebruikte reeksen trainings-, validatie- en testdata, onder meer, indien passend en met inachtneming van beveiligingswaarborgen, via API's of andere relevante technische middelen en instrumenten die toegang op afstand mogelijk maken.

- 4.4. Bij de beoordeling van de technische documentatie kan de aangemelde instantie eisen dat de aanbieder nader bewijs overlegt of nadere tests uitvoert, zodat een passende conformiteitsbeoordeling kan worden uitgevoerd om te controleren of het AI-systeem voldoet aan de eisen van hoofdstuk III, afdeling 2. Indien de aangemelde instantie niet tevreden is met de door de aanbieder uitgevoerde tests, voert de aangemelde instantie zelf toereikende tests uit, voor zover passend.
- 4.5. Indien dat noodzakelijk is om te beoordelen of het AI-systeem met een hoog risico voldoet aan de eisen van hoofdstuk III, afdeling 2, nadat alle andere redelijke manieren om de conformiteit te verifiëren, zijn uitgeput of ontoereikend zijn gebleken, en na een met redenen omkleed verzoek, krijgt de aangemelde instantie eveneens toegang tot de trainings- en getrainde modellen van het AI-systeem, met inbegrip van de relevante parameters ervan. Die toegang is onderworpen aan het bestaande Unierecht inzake de bescherming van intellectuele eigendom en bedrijfsgeheimen.
- 4.6. Het besluit van de aangemelde instantie wordt meegedeeld aan de aanbieder of diens gemachtigde. In deze kennisgeving zijn de conclusies van de beoordeling van de technische documentatie opgenomen, evenals de met redenen omklede beoordelingsbeslissing.

Indien het AI-systeem voldoet aan de eisen van hoofdstuk III, afdeling 2, geeft de aangemelde instantie een beoordelingscertificaat technische documentatie van de Unie af. Het certificaat bevat naam en adres van de aanbieder, de controlebevindingen, de eventuele voorwaarden voor de geldigheid van het certificaat en de noodzakelijke gegevens voor de identificatie van het AI-systeem.

Het certificaat en de bijlagen daarbij bevatten alle relevante informatie voor de evaluatie van de conformiteit van het AI-systeem en maken het mogelijk het in gebruik zijnde AI-systeem te controleren, indien van toepassing.

Indien het AI-systeem niet voldoet aan de eisen van hoofdstuk III, afdeling 2, weigert de aangemelde instantie een beoordelingscertificaat technische documentatie van de Unie te verstrekken en brengt zij de aanvrager hiervan op de hoogte met vermelding van de precieze redenen voor de weigering.

Indien het AI-systeem niet voldoet aan de eis met betrekking tot de gebruikte trainingsdata, moet het AI-systeem opnieuw worden getraind voorafgaand aan de aanvraag voor een nieuwe conformiteitsbeoordeling. In dit geval bevat de met redenen omklede beoordelingsbeslissing van de aangemelde instantie waarin het beoordelingscertificaat technische documentatie van de Unie wordt geweigerd de specifieke overwegingen ten aanzien van de kwaliteitsdata die worden gebruikt voor de training van het AI-systeem, met name over de redenen waarom deze niet voldoen.

- 4.7. Eventuele wijzigingen in het AI-systeem die van invloed kunnen zijn op de naleving door het AI-systeem van de eisen of het beoogde doel, worden beoordeeld door de aangemelde instantie die het beoordelingscertificaat technische documentatie van de Unie heeft verstrekt. De aanbieder informeert die aangemelde instantie over zijn voornemen om een van voornoemde wijzigingen door te voeren of wanneer hij zich anderszins bewust wordt van het bestaan van dergelijke wijzigingen. De aangemelde instantie beoordeelt de voorgenomen wijzigingen en beslist of deze een nieuwe conformiteitsbeoordeling vereisen overeenkomstig artikel 43, lid 4, dan wel of een aanvulling op het beoordelingscertificaat technische documentatie van de Unie volstaat. In het laatste geval beoordeelt de aangemelde instantie de wijzigingen, stelt zij de aanbieder in kennis van haar besluit en verstrekt hem, indien de wijzigingen worden goedgekeurd, een aanvulling op het beoordelingscertificaat technische documentatie van de Unie.

5. Toezicht op het goedgekeurde kwaliteitsbeheersysteem.
- 5.1. Het doel van het door de aangemelde instantie in punt 3 bedoelde uitgevoerde toezicht is te waarborgen dat de aanbieder naar behoren voldoet aan de algemene voorwaarden van het goedgekeurde kwaliteitsbeheersysteem.
- 5.2. De aanbieder stelt de aangemelde instantie in staat om voor beoordelingsdoeleinden toegang te krijgen tot de locatie waar het ontwerp, de ontwikkeling en het testen van de AI-systemen plaatsvindt. De aanbieder deelt voorts alle nodige informatie met de aangemelde instantie.
- 5.3. De aangemelde instantie verricht periodieke audits om te controleren of de aanbieder het kwaliteitsbeheersysteem onderhoudt en toepast en verstrekt de aanbieder een auditverslag. In het kader van deze audits kan de aangemelde instantie aanvullende tests uitvoeren van de AI-systemen waarvoor een beoordelingscertificaat technische documentatie van de Unie is verstrekt.
-

BIJLAGE VIII

Informatie die moet worden verstrekt bij de registratie
van AI-systemen met een hoog risico in overeenstemming met artikel 49

Afdeling A – Informatie die moet worden ingediend door aanbieders van AI-systemen
met een hoog risico overeenkomstig artikel 49, lid 1

Voor wat betreft AI-systemen met een hoog risico die moeten worden geregistreerd in
overeenstemming met artikel 49, lid 1, wordt de volgende informatie verstrekt en daarna actueel
gehouden:

1. de naam, het adres en de contactgegevens van de aanbieder;
2. indien de informatie wordt ingediend door een andere persoon namens de aanbieder, de naam, het adres en de contactgegevens van die persoon;
3. de naam, het adres en de contactgegevens van de gemachtigde, indien van toepassing;
4. de handelsnaam van het AI-systeem, evenals eventuele aanvullende ondubbelzinnige verwijzingen waarmee het AI-systeem kan worden geïdentificeerd en getraceerd;
5. een beschrijving van het beoogde doel van het AI-systeem en van de componenten en functies die door dit AI-systeem worden ondersteund;
6. een basale en beknopte beschrijving van de door het systeem gebruikte informatie (data, input) en de operationele logica ervan;

7. de status van het AI-systeem (in de handel, in gebruik, niet langer in de handel/in gebruik, teruggeroepen);
8. het type, het nummer en de verloopdatum van het door de aangemelde instantie verstrekte certificaat en de naam of het identificatienummer van die aangemelde instantie, indien van toepassing;
9. een gescand exemplaar van het in punt 8 bedoelde certificaat, indien van toepassing;
10. de lidstaten waarin het AI-systeem in de handel is gebracht, in gebruik is gesteld of op de markt in de Unie is aangeboden;
11. een exemplaar van de in artikel 47 bedoelde EU-conformiteitsverklaring;
12. een elektronische gebruiksaanwijzing; deze informatie wordt niet verstrekt voor AI-systemen met een hoog risico op het gebied van rechtshandhaving of migratie-, asiel- en grenstoezichtsbeheer, als bedoeld in bijlage III, punten 1, 6 en 7;
13. een URL voor aanvullende informatie (facultatief).

Afdeling B – Informatie die moet worden ingediend door aanbieders van AI-systemen
met een hoog risico overeenkomstig artikel 49, lid 2

Voor wat betreft AI-systemen met een hoog risico die moeten worden geregistreerd in overeenstemming met artikel 49, lid 2, wordt de volgende informatie verstrekt en daarna actueel gehouden:

1. de naam, het adres en de contactgegevens van de aanbieder;
2. indien de informatie wordt ingediend door een andere persoon namens de aanbieder, de naam, het adres en de contactgegevens van die persoon;
3. de naam, het adres en de contactgegevens van de gemachtigde, indien van toepassing;
4. de handelsnaam van het AI-systeem, evenals eventuele aanvullende ondubbelzinnige verwijzingen waarmee het AI-systeem kan worden geïdentificeerd en getraceerd;
5. een beschrijving van het beoogde doel van het AI-systeem;
6. de voorwaarde of voorwaarden uit hoofde van artikel 6, lid 3, waaronder het AI-systeem niet wordt beschouwd als een systeem met een hoog risico;
7. een korte samenvatting van de redenen waarom het AI-systeem bij de toepassing van de procedure uit hoofde van artikel 6, lid 3, niet als een systeem met een hoog risico wordt beschouwd;
8. de status van het AI-systeem (in de handel, in gebruik, niet langer in de handel/in gebruik, teruggeroepen);
9. de lidstaten waarin het AI-systeem in de handel is gebracht, in gebruik is gesteld of op de markt in de Unie is aangeboden.

Afdeling C – Informatie die moet worden ingediend door gebruiksverantwoordelijken
van AI-systemen met een hoog risico overeenkomstig artikel 49, lid 3

Voor wat betreft AI-systemen met een hoog risico die moeten worden geregistreerd in
overeenstemming met artikel 49, lid 3, wordt de volgende informatie verstrekt en daarna actueel
gehouden:

1. de naam, het adres en de contactgegevens van de gebruiksverantwoordelijke;
2. de naam, het adres en de contactgegevens van de persoon die namens de
gebruiksverantwoordelijke informatie indient;
3. de URL van de invoer van het AI-systeem in de EU-databank door de aanbieder ervan;
4. een samenvatting van de bevindingen van de overeenkomstig artikel 27 uitgevoerde
effectbeoordeling op het gebied van de grondrechten;
5. een samenvatting van de gegevensbeschermingseffectbeoordeling die is uitgevoerd
overeenkomstig artikel 35 van Verordening (EU) 2016/679 of artikel 27 van
Richtlijn (EU) 2016/680, als nader bepaald in artikel 26, lid 8, van deze verordening,
indien van toepassing.

BIJLAGE IX

Informatie die moet worden ingediend bij de registratie van de in bijlage III vermelde AI-systemen met een hoog risico, met betrekking tot tests onder reële omstandigheden overeenkomstig artikel 60

Wat betreft tests onder reële omstandigheden die moeten worden geregistreerd in overeenstemming met artikel 60 wordt de volgende informatie verstrekt en daarna up-to-date gehouden:

1. Een Uniebreed uniek identificatienummer van de tests onder reële omstandigheden;
2. De naam en de contactgegevens van de aanbieder of potentiële aanbieder en van de gebruiksverantwoordelijken die betrokken zijn bij de tests onder reële omstandigheden;
3. Een korte beschrijving van het AI-systeem, het beoogde doel ervan en andere informatie die nodig is voor de identificatie van het systeem;
4. Een samenvatting van de voornaamste kenmerken van het plan voor de tests onder reële omstandigheden;
5. Informatie over het opschorten of beëindigen van tests onder reële omstandigheden.

BIJLAGE X

Wetgevingshandelingen van de Unie over grootschalige IT-systemen in de ruimte van vrijheid, veiligheid en recht

1. Schengeninformatiesysteem

- a) Verordening (EU) 2018/1860 van het Europees Parlement en de Raad van 28 november 2018 betreffende het gebruik van het Schengeninformatiesysteem voor de terugkeer van illegaal verblijvende onderdanen van derde landen (PB L 312 van 7.12.2018, blz. 1);
- b) Verordening (EU) 2018/1861 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van grenscontroles, tot wijziging van de Overeenkomst ter uitvoering van het Akkoord van Schengen en tot wijziging en intrekking van Verordening (EG) nr. 1987/2006 (PB L 312 van 7.12.2018, blz. 14);
- c) Verordening (EU) 2018/1862 van het Europees Parlement en de Raad van 28 november 2018 betreffende de instelling, de werking en het gebruik van het Schengeninformatiesysteem (SIS) op het gebied van politieke en justitiële samenwerking in strafzaken, tot wijziging en intrekking van Besluit 2007/533/JBZ van de Raad en tot intrekking van Verordening (EG) nr. 1986/2006 van het Europees Parlement en de Raad en Besluit 2010/261/EU van de Commissie (PB L 312 van 7.12.2018, blz. 56).

2. Visuminformatiesysteem

- a) Verordening (EU) 2021/1133 van het Europees Parlement en de Raad van 7 juli 2021 tot wijziging van Verordeningen (EU) nr. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 en (EU) 2019/818 wat betreft de voorwaarden voor toegang tot andere EU-informatiesystemen met het oog op het Visuminformatiesysteem (PB L 248 van 13.7.2021, blz. 1);
- b) Verordening (EU) 2021/1134 van het Europees Parlement en de Raad van 7 juli 2021 tot wijziging van de Verordeningen (EG) nr. 767/2008, (EG) nr. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 en (EU) 2019/1896 van het Europees Parlement en de Raad en tot intrekking van Beschikking 2004/512/EG van de Raad en 2008/633/JBZ van de Raad, met het oog op de herziening van het Visuminformatiesysteem (PB L 248 van 13.7.2021, blz. 11).

3. Eurodac

Verordening (EU 2024/... van het Europees Parlement en de Raad betreffende de instelling van “Eurodac” voor de vergelijking van biometrische gegevens om de Verordeningen (EU) 2024/... en (EU) 2024/... van het Europees Parlement en de Raad en Richtlijn 2001/55/EG van de Raad doeltreffend toe te passen en om illegaal verblijvende onderdanen van derde landen en staatlozen te identificeren en betreffende verzoeken van rechtshandavingsinstanties van de lidstaten en Europol om vergelijkingen van Eurodac-gegevens ten behoeve van rechtshandhaving, tot wijziging van de Verordeningen (EU) 2018/1240 en (EU) 2019/818 van het Europees Parlement en de Raad en tot intrekking van Verordening (EU) nr. 603/2013 van het Europees Parlement en de Raad⁺.

4. Inreis-uitreisysteem

Verordening (EU) 2017/2226 van het Europees Parlement en de Raad van 30 november 2017 tot instelling van een inreis-uitreisysteem (EES) voor de registratie van inreis- en uitreisgegevens en van gegevens over weigering van toegang ten aanzien van onderdanen van derde landen die de buitengrenzen overschrijden en tot vaststelling van de voorwaarden voor toegang tot het EES voor rechtshandavingsdoeleinden en tot wijziging van de overeenkomst ter uitvoering van het te Schengen gesloten akkoord en Verordeningen (EG) nr. 767/2008 en (EU) nr. 1077/2011 (PB L 327 van 9.12.2017, blz. 20).

⁺ PB: gelieve in de tekst het nummer van de verordening in document PE-CONS 15/24 (2016/0132(COD)) in te voegen, en het nummer, de datum, de titel en de verwijzing naar het PB van die verordening in de voetnoot in te voegen.

5. Europees systeem voor reisinformatie en -autorisatie
- a) Verordening (EU) 2018/1240 van het Europees Parlement en de Raad van 12 september 2018 tot oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) en tot wijziging van de Verordeningen (EU) nr. 1077/2011, (EU) nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 en (EU) 2017/2226 (PB L 236 van 19.9.2018, blz. 1);
 - b) Verordening (EU) 2018/1241 van het Europees Parlement en de Raad van 12 september 2018 tot wijziging van Verordening (EU) 2016/794 met het oog op de oprichting van een Europees reisinformatie- en -autorisatiesysteem (Etias) (PB L 236 van 19.9.2018, blz. 72).
6. Europees Strafregisterinformatiesysteem over onderdanen van derde landen en staatlozen
- Verordening (EU) 2019/816 van het Europees Parlement en de Raad van 17 april 2019 tot invoering van een gecentraliseerd systeem voor de vaststelling welke lidstaten over informatie beschikken inzake veroordelingen van onderdanen van derde landen en staatlozen (Ecris-TCN) ter aanvulling van het Europees Strafregisterinformatiesysteem en tot wijziging van Verordening (EU) 2018/1726 (PB L 135 van 22.5.2019, blz. 1).

7. Interoperabiliteit

- a) Verordening (EU) 2019/817 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van grenzen en visa en tot wijziging van Verordeningen (EG) nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 en (EU) 2018/1861 van het Europees Parlement en de Raad, Beschikking 2004/512/EG van de Raad en Besluit 2008/633/JBZ van de Raad (PB L 135 van 22.5.2019, blz. 27);
 - b) Verordening (EU) 2019/818 van het Europees Parlement en de Raad van 20 mei 2019 tot vaststelling van een kader voor interoperabiliteit tussen de Unie-informatiesystemen op het gebied van politieke en justitiële samenwerking, asiel en migratie en tot wijziging van Verordeningen (EU) 2018/1726, (EU) 2018/1862 en (EU) 2019/816 (PB L 135 van 22.5.2019, blz. 85).
-

BIJLAGE XI

Technische documentatie als bedoeld in artikel 53, lid 1, punt a) - technische documentatie
voor aanbieders van AI-modellen voor algemene doeleinden

Afdeling 1

Informatie die moet worden verstrekt door alle aanbieders van ai-modellen
voor algemene doeleinden

De technische documentatie als bedoeld in artikel 53, lid 1, punt a), bevat ten minste de volgende informatie, naargelang van de omvang en het risicoprofiel van het model:

1. Een algemene beschrijving van het AI-model voor algemene doeleinden, met daarin:
 - a) de taken die het model moet uitvoeren en het type en de aard van AI-systemen waarin het kan worden geïntegreerd;
 - b) de “acceptable use policies” die van toepassing zijn;
 - c) de releasedatum en de wijze van verspreiding;
 - d) de architectuur en het aantal parameters;
 - e) de modaliteit (bv. tekst, afbeelding) en het formaat van de input en output;
 - f) de licentie.

2. Een gedetailleerde beschrijving van de elementen van het in punt 1 bedoelde model en relevante informatie over het ontwikkelingsproces, met inbegrip van de volgende elementen:
- a) de technische middelen (bv. gebruiksinstructies, infrastructuur, instrumenten) die nodig zijn voor de integratie van het AI-model voor algemene doeleinden in AI-systemen;
 - b) de specificaties van het ontwerp van het model en het trainingsproces, met inbegrip van trainingsmethoden en -technieken, de belangrijkste ontwerpkeuzes, met inbegrip van de motivering en de gemaakte aannames; voor welke optimalisatie het model is ontworpen en de relevantie van de verschillende parameters, naargelang van het geval;
 - c) informatie over de data die zijn gebruikt voor training, tests en validatie, indien van toepassing, met inbegrip van het type en de herkomst van de data en curatiemethoden (bv. schoonmaken, filteren enz.), het aantal datapunten, hun bereik en belangrijkste kenmerken; de wijze waarop de data zijn verkregen en geselecteerd, alsmede alle andere maatregelen om de ongeschiktheid van databronnen te detecteren, en methoden voor het opsporen van identificeerbare vooroordelen, indien van toepassing;
 - d) de rekenhulpmiddelen die zijn gebruikt om het model te trainen (bv. aantal zwevendekomma bewerkingen), de duur en andere relevante bijzonderheden over de training;
 - e) bekend of geraamd energieverbruik van het model.

Met betrekking tot punt e) kan, indien het energieverbruik van het model onbekend is, het energieverbruik gebaseerd zijn op informatie over de gebruikte rekenhulpmiddelen.

Afdeling 2

Aanvullende informatie die moet worden verstrekt door aanbieders van AI-modellen met een systeemrisico

1. Een gedetailleerde beschrijving van de evaluatiestrategieën, met inbegrip van evaluatieresultaten, op basis van beschikbare openbare evaluatieprotocollen en -instrumenten of andere evaluatiemethoden. De evaluatiestrategieën omvatten evaluatiecriteria, maatstaven en de methoden voor het in kaart brengen van beperkingen.
 2. Indien van toepassing, een gedetailleerde beschrijving van de maatregelen die zijn genomen met het oog op het uitvoeren van interne en/of externe tests gericht op het ontdekken van kwetsbaarheden (bv. red teaming), modelaanpassingen, inclusief afstemming en verfijning.
 3. Indien van toepassing, een gedetailleerde beschrijving van de systeemarchitectuur met een toelichting bij hoe softwarecomponenten op elkaar voortbouwen of elkaar informatie aanleveren en hoe de integratie in de algemene verwerking plaatsvindt.
-

BIJLAGE XII

Transparantie-informatie als bedoeld in artikel 53, lid 1, punt b) - technische documentatie
voor aanbieders van AI-modellen voor algemene doeleinden
aan aanbieders verder in de AI-waardeketen die het model in hun AI-systeem integreren

De in artikel 53, lid 1, punt b), bedoelde informatie omvat ten minste de volgende elementen:

1. Een algemene beschrijving van het AI-model voor algemene doeleinden, met daarin:
 - a) de taken die het model moet uitvoeren en het type en de aard van AI-systemen waarin het kan worden geïntegreerd;
 - b) de “acceptable use policies” die van toepassing zijn;
 - c) de releasedatum en de wijze van verspreiding;
 - d) hoe het model interageert of kan worden gebruikt om te interageren met hardware of software die geen deel uitmaakt van het model zelf, indien van toepassing;
 - e) de versies van relevante software met betrekking tot het gebruik van het AI-model voor algemene doeleinden, indien van toepassing;
 - f) de architectuur en het aantal parameters;
 - g) de modaliteit (bv. tekst, afbeelding) en het formaat van de input en output;
 - h) de licentie voor het model.

2. Een beschrijving van de elementen van het model en van het proces voor de ontwikkeling ervan, waaronder:
- a) de technische middelen (bv. gebruiksinstructies, infrastructuur, instrumenten) die nodig zijn voor de integratie van het AI-model voor algemene doeleinden in AI-systemen;
 - b) de modaliteit (bv. tekst, afbeelding enz.) en het formaat van de input en output en de maximale omvang ervan (bv. lengte van het contextvenster enz.);
 - c) informatie over de data die worden gebruikt voor training, tests en validatie, indien van toepassing, met inbegrip van het type en de herkomst van de data en curatiemethoden.
-

BIJLAGE XIII

In artikel 51 bedoelde criteria voor de aanwijzing van AI-modellen
voor algemene doeleinden met een systeemrisico

Om te bepalen of een AI-model voor algemene doeleinden capaciteiten of een impact heeft die vergelijkbaar zijn met die welke zijn vermeld in artikel 51, lid 1, punt a), houdt de Commissie rekening met de volgende criteria:

- a) het aantal parameters van het model;
- b) de kwaliteit of omvang van de dataset, bijvoorbeeld gemeten aan de hand van tokens;
- c) de hoeveelheid rekenhulpmiddelen die is gebruikt om het model te trainen, gemeten in zwevendekomma bewerkingen, of uitgedrukt door een combinatie van andere variabelen, zoals de geraamde kosten, tijd of energieverbruik voor de opleiding;
- d) de input- en outputmodaliteiten van het model, zoals tekst-naar-tekst (grote taalmodellen), tekst-naar-beeld, multimodaliteit, en de geavanceerde drempels voor het bepalen van capaciteiten met een grote impact voor elke modaliteit, en het specifieke type input en output (bv. biologische sequenties);
- e) de benchmarks en evaluaties van de capaciteiten van het model, met inbegrip van het aantal taken zonder aanvullende training, het aanpassingsvermogen om nieuwe, afzonderlijke taken te leren, de mate van autonomie en schaalbaarheid en de instrumenten waartoe het toegang heeft;

- f) of het een grote impact heeft op de interne markt vanwege het bereik ervan, wat verondersteld wordt wanneer het beschikbaar is gesteld aan ten minste 10 000 geregistreerde zakelijke gebruikers die in de Unie zijn gevestigd;
 - g) het aantal geregistreerde eindgebruikers.”.
-

RECTIFICARE

**la Regulamentul (UE) al Parlamentului European și al Consiliului din 13 iunie 2024 de
stabilire a unor norme armonizate privind inteligența artificială și de modificare a
Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE)
2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828
(Regulamentul privind inteligența artificială)**

(PE-CONS 24/1/24 REV 1, 14 iunie 2024)

Regulamentul cuprins în documentul PE-CONS 24/1/24 REV 1 se citește după cum urmează:

REGULAMENTUL (UE) 2024/...
AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

din 13 iunie 2024

**de stabilire a unor norme armonizate privind inteligența artificială
și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013,
(UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144
și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828
(Regulamentul privind inteligența artificială)**

(Text cu relevanță pentru SEE)

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolele 16 și 114,

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European¹,

având în vedere avizul Băncii Centrale Europene²,

având în vedere avizul Comitetului Regiunilor³,

hotărând în conformitate cu procedura legislativă ordinară⁴,

¹ JO C 517, 22.12.2021, p. 56.

² JO C 115, 11.3.2022, p. 5.

³ JO C 97, 28.2.2022, p. 60.

⁴ Poziția Parlamentului European din 13 martie 2024 (nepublicată încă în Jurnalul Oficial) și Decizia Consiliului din 21 mai 2024.

întrucât:

- (1) Scopul prezentului regulament este de a îmbunătăți funcționarea pieței interne prin stabilirea unui cadru juridic uniform, în special pentru dezvoltarea, introducerea pe piață, punerea în funcțiune și utilizarea de sisteme de inteligență artificială (sisteme de IA) în Uniune, în conformitate cu valorile Uniunii, de a promova adoptarea unei inteligențe artificiale (IA) de încredere și centrate pe factorul uman, asigurând în același timp un nivel ridicat de protecție a sănătății, a siguranței, a drepturilor fundamentale consacrate în Carta drepturilor fundamentale a Uniunii Europene (denumită în continuare „Carta”), inclusiv a democrației, a statului de drept și a mediului, de a proteja împotriva efectelor dăunătoare ale sistemelor de IA în Uniune, precum și de a sprijini inovarea. Prezentul regulament asigură libera circulație transfrontalieră a bunurilor și serviciilor bazate pe IA, împiedicând astfel statele membre să impună restricții privind dezvoltarea, comercializarea și utilizarea sistemelor de IA, cu excepția cazului în care acest lucru este autorizat în mod explicit de prezentul regulament.
- (2) Prezentul regulament ar trebui să se aplice în conformitate cu valorile Uniunii consacrate în cartă, facilitând protecția persoanelor fizice, a întreprinderilor, a democrației, a statului de drept și a mediului, stimulând în același timp inovarea și ocuparea forței de muncă și asigurând Uniunii o poziție de lider în adoptarea unei IA de încredere.

- (3) Sistemele de IA pot fi implementate cu ușurință într-o mare varietate de sectoare ale economiei și în multe părți ale societății, inclusiv la nivel transfrontalier, și pot circula cu ușurință în întreaga Uniune. Anumite state membre au explorat deja adoptarea unor norme naționale pentru a se asigura că IA este sigură și de încredere și că este dezvoltată și utilizată în conformitate cu obligațiile în materie de drepturi fundamentale. Divergențele dintre normele naționale pot duce la fragmentarea pieței interne și pot reduce gradul de securitate juridică pentru operatorii care dezvoltă, importă sau utilizează sisteme de IA. Prin urmare, ar trebui să se asigure un nivel ridicat și consecvent de protecție în întreaga Uniune pentru a se obține o IA de încredere, iar divergențele care împiedică libera circulație, inovarea, implementarea și adoptarea sistemelor de IA și a produselor și serviciilor conexe în cadrul pieței interne ar trebui să fie prevenite, prin stabilirea unor obligații uniforme pentru operatori și prin garantarea protecției uniforme a motivelor imperative de interes public major și a drepturilor persoanelor în întreaga piață internă, în temeiul articolului 114 din Tratatul privind funcționarea Uniunii Europene (TFUE). În măsura în care prezentul regulament conține norme specifice de protecție a persoanelor fizice în contextul prelucrării datelor cu caracter personal, referitoare la restricțiile de utilizare a sistemelor de IA pentru identificarea biometrică la distanță în scopul aplicării legii, la utilizarea sistemelor de IA pentru evaluarea riscurilor persoanelor fizice în scopul aplicării legii și la utilizarea sistemelor de IA de clasificare biometrică în scopul aplicării legii, este oportun ca prezentul regulament să se întemeieze, în ceea ce privește normele specifice respective, pe articolul 16 din TFUE. Având în vedere normele specifice respective și recurgerea la articolul 16 din TFUE, este oportun să se consulte Comitetul european pentru protecția datelor.

- (4) IA este o familie de tehnologii cu evoluție rapidă, care contribuie la o gamă largă de beneficii economice, de mediu și societale în întregul spectru de industrii și activități sociale. Prin îmbunătățirea previziunilor, optimizarea operațiunilor și a alocării resurselor, precum și prin personalizarea soluțiilor digitale disponibile pentru persoane fizice și organizații, utilizarea IA poate oferi avantaje concurențiale esențiale întreprinderilor și poate sprijini obținerea de rezultate benefice din punct de vedere social și al mediului, în domenii precum îngrijirile de sănătate, agricultura, siguranța alimentară, educația și formarea, mass-media, sportul, cultura, gestionarea infrastructurii, energia, transporturile și logistica, serviciile publice, securitatea, justiția, eficiența energetică și a utilizării resurselor, monitorizarea mediului, conservarea și refacerea biodiversității și ecosistemelor, precum și atenuarea schimbărilor climatice și adaptarea la acestea.
- (5) În același timp, în funcție de circumstanțele legate de aplicarea și utilizarea sa specifică, precum și de nivelul său specific de dezvoltare tehnologică, IA poate genera riscuri și poate aduce prejudicii intereselor publice și drepturilor fundamentale care sunt protejate de dreptul Uniunii. Un astfel de prejudiciu ar putea fi material sau moral, inclusiv de natură fizică, psihologică, societală sau economică.

- (6) Având în vedere impactul major pe care IA îl poate avea asupra societății și necesitatea de a genera încredere, este esențial ca IA și cadrul său de reglementare să fie dezvoltate în concordanță cu valorile Uniunii consacrate la articolul 2 din Tratatul privind Uniunea Europeană (TUE) și cu drepturile și libertățile fundamentale consacrate în tratate și, potrivit articolului 6 din TUE, în Cartă. Ca o condiție prealabilă, IA ar trebui să fie o tehnologie centrată pe factorul uman. Aceasta ar trebui să le servească oamenilor ca un instrument, cu scopul final de a le spori bunăstarea.
- (7) Pentru a asigura un nivel consecvent și ridicat de protecție a intereselor publice în ceea ce privește sănătatea, siguranța și drepturile fundamentale, ar trebui să fie stabilite norme comune pentru sistemele de IA cu grad ridicat de risc. Normele respective ar trebui să fie în concordanță cu cartă și ar trebui să fie nediscriminatorii și în conformitate cu angajamentele comerciale internaționale ale Uniunii. De asemenea, ele ar trebui să țină seama de Declarația europeană privind drepturile și principiile digitale pentru deceniul digital și de Orientările în materie de etică pentru o IA fiabilă ale Grupului independent de experți la nivel înalt privind inteligența artificială.

- (8) Prin urmare, este necesar un cadru juridic al Uniunii care să stabilească norme armonizate privind IA pentru a încuraja dezvoltarea, utilizarea și adoptarea pe piața internă a IA și care să asigure, în același timp, un nivel ridicat de protecție a intereselor publice, cum ar fi sănătatea și siguranța, și protecția drepturilor fundamentale, inclusiv a democrației, a statului de drept și a mediului, astfel cum sunt recunoscute și protejate de dreptul Uniunii. Pentru atingerea acestui obiectiv, ar trebui să fie stabilite norme care să reglementeze introducerea pe piață, punerea în funcțiune și utilizarea anumitor sisteme de IA, asigurând astfel buna funcționare a pieței interne și permițând sistemelor respective să beneficieze de principiul liberei circulații a bunurilor și a serviciilor. Normele respective ar trebui să fie clare și solide în ceea ce privește protejarea drepturilor fundamentale, sprijinind noile soluții inovatoare, permițând unui ecosistem european de actori publici și privați să creeze sisteme de IA în conformitate cu valorile Uniunii și deblocând potențialul transformării digitale în toate regiunile Uniunii. Prin stabilirea normelor respective, precum și a unor măsuri de susținere a inovării cu un accent special pe întreprinderile mici și mijlocii (IMM), inclusiv pe întreprinderile nou-înființate, prezentul regulament sprijină obiectivul de promovare a abordării europene centrate pe factorul uman față de IA și de poziționare ca lider mondial în dezvoltarea unei IA sigure, de încredere și etice, astfel cum a afirmat Consiliul European⁵, și asigură protecția principiilor etice, astfel cum a solicitat în mod expres Parlamentul European⁶.

⁵ Consiliul European, Reuniunea extraordinară a Consiliului European (1-2 octombrie 2020) – Concluzii, EUCO 13/20, 2020, p. 6.

⁶ Rezoluția Parlamentului European din 20 octombrie 2020 conținând recomandări adresate Comisiei privind cadrul de aspecte etice asociate cu inteligența artificială, robotica și tehnologiile conexe, 2020/2012(INL).

- (9) Normele armonizate aplicabile introducerii pe piață, punerii în funcțiune și utilizării sistemelor de IA cu grad ridicat de risc ar trebui să fie stabilite în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului⁷, cu Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului⁸ și cu Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului⁹ (denumite în continuare „noul cadru legislativ”). Normele armonizate prevăzute în prezentul regulament ar trebui să se aplice în toate sectoarele și, în conformitate cu noul cadru legislativ, ar trebui să nu aducă atingere dreptului în vigoare al Uniunii, în special în ceea ce privește protecția datelor, protecția consumatorilor, drepturile fundamentale, ocuparea forței de muncă, protecția lucrătorilor și siguranța produselor, cu care prezentul regulament este complementar. În consecință, toate drepturile și căile de atac prevăzute de dreptul Uniunii pentru consumatori și alte persoane asupra cărora sistemele de IA ar putea avea un impact negativ, inclusiv în ceea ce privește despăgubirea pentru eventuale prejudicii prevăzută în Directiva 85/374/CEE a Consiliului¹⁰, rămân neafectate și pe deplin aplicabile.

⁷ Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a cerințelor de acreditare și de abrogare a Regulamentului (CEE) nr. 339/93 (JO L 218, 13.8.2008, p. 30).

⁸ Decizia nr. 768/2008/CE a Parlamentului European și a Consiliului din 9 iulie 2008 privind un cadru comun pentru comercializarea produselor și de abrogare a Deciziei 93/465/CEE a Consiliului (JO L 218, 13.8.2008, p. 82).

⁹ Regulamentul (UE) 2019/1020 al Parlamentului European și al Consiliului din 20 iunie 2019 privind supravegherea pieței și conformitatea produselor și de modificare a Directivei 2004/42/CE și a Regulamentelor (CE) nr. 765/2008 și (UE) nr. 305/2011 (JO L 169, 25.6.2019, p. 1).

¹⁰ Directiva 85/374/CEE a Consiliului din 25 iulie 1985 de apropiere a actelor cu putere de lege și a actelor administrative ale statelor membre cu privire la răspunderea pentru produsele cu defect (JO L 210, 7.8.1985, p. 29).

În plus, în contextul ocupării forței de muncă și al protecției lucrătorilor, prezentul regulament ar trebui așadar să nu aducă atingere dreptului Uniunii privind politica socială și dreptului național al muncii, în conformitate cu dreptul Uniunii, în ceea ce privește condițiile de angajare și de muncă, inclusiv securitatea și sănătatea în muncă și relația dintre angajatori și lucrători. De asemenea, prezentul regulament ar trebui să nu aducă atingere exercitării drepturilor fundamentale, astfel cum sunt recunoscute în statele membre și la nivelul Uniunii, inclusiv dreptului sau libertății de a intra în grevă sau de a întreprinde alte acțiuni care țin de sistemele specifice de relații de muncă din statele membre, precum și dreptului de a negocia, de a încheia și de a pune în aplicare contracte colective de muncă sau de a desfășura acțiuni colective în conformitate cu dreptul intern. Prezentul regulament ar trebui să nu aducă atingere dispozițiilor care vizează îmbunătățirea condițiilor de muncă în ceea ce privește munca prin intermediul platformelor, prevăzute într-o Directivă a Parlamentului European și a Consiliului privind îmbunătățirea condițiilor de muncă pentru lucrul prin intermediul platformelor. În plus, prezentul regulament urmărește să consolideze eficacitatea acestor drepturi și căi de atac existente prin stabilirea unor cerințe și obligații specifice, inclusiv în ceea ce privește transparența, documentația tehnică și păstrarea evidențelor sistemelor de IA. De asemenea, obligațiile impuse diferiților operatori implicați în lanțul valoric al IA în temeiul prezentului regulament ar trebui să se aplice fără a aduce atingere dreptului intern, în conformitate cu dreptul Uniunii, având ca efect limitarea utilizării anumitor sisteme de IA în cazul în care dreptul respectiv nu intră în domeniul de aplicare al prezentului regulament sau urmărește alte obiective legitime de interes public decât cele urmărite de prezentul regulament. De exemplu, dreptul intern al muncii și dreptul intern privind protecția minorilor, și anume a persoanelor cu vârsta sub 18 ani, ținând seama de Comentariul general nr. 25 (2021) la Convenția UNCRC cu privire la drepturile copiilor în legătură cu mediul digital, în măsura în care nu sunt specifice sistemelor de IA și urmăresc alte obiective legitime de interes public, ar trebui să nu fie afectate de prezentul regulament.

- (10) Dreptul fundamental la protecția datelor cu caracter personal este protejat în special de Regulamentele (UE) 2016/679¹¹ și (UE) 2018/1725¹² ale Parlamentului European și ale Consiliului și de Directiva (UE) 2016/680 a Parlamentului European și a Consiliului¹³. Directiva 2002/58/CE a Parlamentului European și a Consiliului¹⁴ protejează, în plus, viața privată și confidențialitatea comunicațiilor, inclusiv prin faptul că prevede condiții pentru stocarea și accesarea pe echipamente terminale a oricăror date cu și fără caracter personal. Respectivele acte legislative ale Uniunii asigură temeiul prelucrării durabile și responsabile a datelor, inclusiv atunci când seturile de date conțin un amestec de date cu caracter personal și date fără caracter personal. Prezentul regulament nu urmărește să aducă atingere aplicării dreptului în vigoare al Uniunii care reglementează prelucrarea datelor cu caracter personal, nici sarcinilor și competențelor autorităților de supraveghere independente care sunt competente să monitorizeze respectarea instrumentelor respective.

¹¹ Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

¹² Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39).

¹³ Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

¹⁴ Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

Prezentul regulament nu aduce atingere nici obligațiilor furnizorilor și implementatorilor de sisteme de IA în rolul lor de operatori de date sau de persoane împuternicite de operatori, care decurg din dreptul Uniunii sau din dreptul național privind protecția datelor cu caracter personal, în măsura în care proiectarea, dezvoltarea sau utilizarea sistemelor de IA implică prelucrarea de date cu caracter personal. De asemenea, este oportun să se clarifice că persoanele vizate continuă să beneficieze de toate drepturile și garanțiile care le sunt acordate de dreptul Uniunii, printre care se numără drepturile legate de procesul decizional individual complet automatizat, inclusiv crearea de profiluri. Normele armonizate pentru introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA instituite în temeiul prezentului regulament ar trebui să faciliteze punerea în aplicare efectivă și să permită exercitarea drepturilor persoanelor vizate și a altor căi de atac garantate în temeiul dreptului Uniunii privind protecția datelor cu caracter personal și a altor drepturi fundamentale.

- (11) Prezentul regulament ar trebui să nu aducă atingere dispozițiilor privind răspunderea furnizorilor de servicii intermediare prevăzute în Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului¹⁵.

¹⁵ Regulamentul (UE) 2022/2065 al Parlamentului European și al Consiliului din 19 octombrie 2022 privind o piață unică pentru serviciile digitale și de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale) (JO L 277, 27.10.2022, p. 1).

- (12) Noțiunea de „sistem de IA” din prezentul regulament ar trebui să fie definită în mod clar și ar trebui să fie aliniată îndeaproape la lucrările organizațiilor internaționale care își desfășoară activitatea în domeniul IA, pentru a asigura securitatea juridică și a facilita convergența internațională și acceptarea pe scară largă, oferind în același timp flexibilitatea necesară pentru a ține seama de evoluțiile tehnologice rapide din acest domeniu. În plus, definiția ar trebui să se bazeze pe caracteristicile esențiale ale sistemelor de IA, care le diferențiază de sistemele software sau abordările de programare tradiționale mai simple, și nu ar trebui să acopere sistemele care se bazează pe reguli definite exclusiv de persoane fizice pentru a executa în mod automat anumite operațiuni. O caracteristică esențială a sistemelor de IA este capacitatea lor de a realiza deducții. Această capacitate se referă la procesul de obținere a rezultatelor, cum ar fi previziuni, conținut, recomandări sau decizii, care pot influența mediile fizice și virtuale, precum și la capacitatea sistemelor de IA de a deriva modele sau algoritmi, sau ambele, din date sau din datele de intrare. Printre tehnicile folosite în timpul conceperii unui sistem de IA care fac posibilă realizarea de deducții se numără abordările bazate pe învățarea automată, care presupun a învăța, pe baza datelor, cum pot fi atinse anumite obiective, și abordările bazate pe logică și pe cunoaștere, care presupun realizarea de deducții pornind de la cunoștințe codificate sau de la reprezentarea simbolică a sarcinii de rezolvat. Capacitatea unui sistem de IA de a realiza deducții depășește simpla prelucrare de date, făcând posibile învățarea, raționamentul sau modelarea. Termenul „bazat pe calculator” se referă la faptul că sistemele de IA rulează pe calculatoare.

Trimiterea la obiective explicite sau implicite subliniază faptul că sistemele de IA pot funcționa în conformitate cu obiective definite explicite sau cu obiective implicite. Obiectivele sistemului de IA pot fi diferite de scopul preconizat al sistemului de IA într-un context specific. În sensul prezentului regulament, mediile ar trebui să fie înțelese ca fiind contextele în care funcționează sistemele de IA, în timp ce rezultatele generate de sistemele de IA reflectă diferitele funcții îndeplinite de acestea și includ previziuni, conținut, recomandări sau decizii. Sistemele de IA sunt concepute pentru a funcționa cu diferite niveluri de autonomie, ceea ce înseamnă că au un anumit grad de independență a acțiunilor față de implicarea umană și anumite capacități de a funcționa fără intervenție umană. Adaptabilitatea de care un sistem de IA ar putea da dovadă după implementare se referă la capacitățile de autoînvățare, care permit sistemului să se modifice în timpul utilizării. Sistemele de IA pot fi utilizate în mod independent sau ca o componentă a unui produs, indiferent dacă sistemul este integrat fizic în produs (încorporat) sau dacă servește funcționalității produsului fără a fi integrat în acesta (neîncorporat).

- (13) Noțiunea de „implementator” menționată în prezentul regulament ar trebui să fie interpretată ca făcând referire la orice persoană fizică sau juridică, inclusiv la o autoritate publică, o agenție sau un alt organism, care utilizează un sistem de IA aflat sub autoritatea sa, cu excepția cazului în care sistemul de IA este utilizat în cursul unei activități personale, fără caracter profesional. În funcție de tipul de sistem de IA, utilizarea sistemului poate afecta alte persoane decât implementatorul.
- (14) Noțiunea de „date biometrice” utilizată în prezentul regulament ar trebui să fie interpretată în concordanță cu noțiunea de „date biometrice”, astfel cum este definită la articolul 4 punctul 14 din Regulamentul (UE) 2016/679, la articolul 3 punctul 18 din Regulamentul (UE) 2018/1725 și la articolul 3 punctul 13 din Directiva (UE) 2016/680. Datele biometrice pot permite autentificarea, identificarea sau clasificarea persoanelor fizice, precum și recunoașterea emoțiilor acestora.
- (15) Noțiunea de „identificare biometrică” menționată în prezentul regulament ar trebui să fie definită drept recunoașterea automată a unor trăsături umane fizice, fiziologice și comportamentale, precum fața, mișcările ochilor, forma corpului, vocea, intonația, mersul, postura, frecvența cardiacă, tensiunea arterială, mirosul, particularitățile de tastare, în scopul de a stabili identitatea unei persoane comparând datele biometrice ale persoanei respective cu date biometrice ale unor persoane stocate într-o bază de date de referință, indiferent dacă persoana în cauză și-a dat sau nu consimțământul. Nu se încadrează aici sistemele de IA destinate a fi utilizate pentru verificarea biometrică, care include autentificarea, al căror unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este și de a confirma identitatea unei persoane fizice cu unicul scop de a-i permite accesul la un serviciu, deblocarea unui dispozitiv sau accesul securizat într-o incintă.

- (16) Noțiunea de „clasificare biometrică” menționată în prezentul regulament ar trebui să fie definită drept încadrarea persoanelor fizice în categorii specifice pe baza datelor lor biometrice. Astfel de categorii specifice se pot referi la aspecte precum sexul, vârsta, culoarea părului, culoarea ochilor, tatuajele, trăsăturile comportamentale sau de personalitate, limba, religia, apartenența la o minoritate națională, orientarea sexuală sau politică. Nu se încadrează aici sistemele de clasificare biometrică care constituie un element pur auxiliar legat intrinsec de un alt serviciu comercial, ceea ce înseamnă că, din motive tehnice obiective, elementul respectiv nu poate fi utilizat fără serviciul principal, iar integrarea acelui element sau a acelei funcționalități nu este un mijloc de a eluda aplicabilitatea normelor prezentului regulament. De exemplu, filtrele care clasifică caracteristicile faciale sau corporale utilizate pe piețele online ar putea constitui un astfel de element auxiliar, deoarece pot fi utilizate numai în legătură cu serviciul principal care constă în vânzarea unui produs, permițând consumatorului să vizualizeze cum ar arăta produsul pe el însuși și ajutându-l să ia o decizie de cumpărare. Filtrele utilizate în cadrul serviciilor de rețele de socializare care clasifică caracteristicile faciale sau corporale pentru a permite utilizatorilor să adauge sau să modifice fotografii sau materiale video ar putea, de asemenea, să fie considerate elemente auxiliare, deoarece un astfel de filtru nu poate fi utilizat fără serviciul principal de rețea de socializare care constă în partajarea de conținut online.

- (17) Noțiunea de „sistem de identificare biometrică la distanță” menționată în prezentul regulament ar trebui să fie definită din punct de vedere funcțional ca fiind un sistem de IA destinat identificării persoanelor fizice fără implicarea activă a acestora, de regulă de la distanță, prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință, indiferent de tehnologia specifică, procesele specifice sau tipurile specifice de date biometrice utilizate. Astfel de sisteme de identificare biometrică la distanță sunt utilizate, de regulă, pentru a percepe mai multe persoane sau comportamentul acestora simultan, cu scopul de a facilita în mod semnificativ identificarea persoanelor fizice fără implicarea lor activă. Nu se încadrează aici sistemele de IA destinate a fi utilizate pentru verificarea biometrică, care include autentificarea, al căror unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este și de a confirma identitatea unei persoane fizice cu unicul scop de a-i permite accesul la un serviciu, deblocarea unui dispozitiv sau accesul securizat într-o încălț. Această excludere este justificată de faptul că, cel mai probabil, astfel de sisteme au un impact minor asupra drepturilor fundamentale ale persoanelor fizice în comparație cu sistemele de identificare biometrică la distanță care pot fi utilizate pentru prelucrarea datelor biometrice ale unui număr mare de persoane fără implicarea lor activă. În cazul sistemelor „în timp real”, captarea datelor biometrice, compararea și identificarea se efectuează instantaneu, aproape instantaneu sau, în orice caz, fără întârzieri semnificative. În acest sens, nu ar trebui să existe posibilități de eludare a normelor prezentului regulament privind utilizarea „în timp real” a sistemelor de IA în cauză prin prevederea unor întârzieri minore. Sistemele „în timp real” implică utilizarea de materiale „în direct” sau „aproape în direct”, cum ar fi înregistrări video generate de o cameră video sau de un alt dispozitiv cu funcționalitate similară. În schimb, în cazul sistemelor de identificare „ulterioară”, datele biometrice au fost deja captate, iar compararea și identificarea au loc numai după o întârziere semnificativă. În acest caz sunt utilizate materiale, cum ar fi imagini sau înregistrări video generate de camere de televiziune cu circuit închis sau de dispozitive private, care au fost generate înainte de utilizarea sistemului în legătură cu persoanele fizice în cauză.

- (18) Noțiunea de „sistem de recunoaștere a emoțiilor” menționată în prezentul regulament ar trebui să fie definită ca un sistem de IA destinat identificării sau deducerii emoțiilor sau intențiilor persoanelor fizice pe baza datelor lor biometrice. Noțiunea se referă la emoții sau intenții precum fericirea, tristețea, furia, surpriza, dezgustul, stânjeneala, entuziasmul, rușinea, disprețul, satisfacția și amuzamentul. Nu sunt incluse stări fizice, cum ar fi durerea sau oboseala, inclusiv, de exemplu, sistemele utilizate pentru detectarea stării de oboseală a piloților sau conducătorilor auto profesioniști în scopul prevenirii accidentelor. De asemenea, nu este inclusă simpla detectare a expresiilor, gesturilor sau mișcărilor evidente, decât dacă sunt utilizate pentru identificarea sau deducerea emoțiilor. Expresiile respective pot fi expresii faciale de bază, cum ar fi o încruntătură sau un zâmbet, ori gesturi, cum ar fi mișcarea mâinilor, a brațelor sau a capului, ori caracteristici ale vocii unei persoane, cum ar fi o voce ridicată sau vorbitul în șoaptă.

- (19) În sensul prezentului regulament, noțiunea de „spațiu accesibil publicului” ar trebui să fie înțeleasă ca referindu-se la orice spațiu fizic accesibil unui număr nedeterminat de persoane fizice, indiferent dacă spațiul în cauză este proprietate privată sau publică și indiferent de activitatea pentru care poate fi utilizat spațiul, cum ar fi comerț, de exemplu, magazine, restaurante, cafenele; servicii, de exemplu, bănci, activități profesionale, structuri de primire turistică; sport, de exemplu, piscine, săli de sport, stadioane; transporturi, de exemplu, stații de autobuz și de metrou, gări, aeroporturi, mijloace de transport; divertisment, de exemplu, cinematografe, teatre, muzee, săli de concerte și de conferințe, agrement sau altele, de exemplu, drumuri și piețe publice, parcuri, păduri, terenuri de joacă. Totodată, un spațiu ar trebui să fie clasificat ca fiind accesibil publicului și în cazul în care, indiferent de capacitatea potențială sau de restricțiile de securitate, accesul este supus anumitor condiții prestabilite, care pot fi îndeplinite de un număr nedeterminat de persoane, cum ar fi achiziționarea unui bilet sau a unui titlu de transport, înregistrarea prealabilă sau condiția de a avea o anumită vârstă. În schimb, un spațiu nu ar trebui să fie considerat accesibil publicului dacă accesul este limitat la anumite persoane fizice definite ca atare fie prin dreptul Uniunii, fie prin cel intern, în legătură directă cu siguranța sau securitatea publică sau prin manifestarea clară de voință a persoanei care deține autoritatea necesară asupra spațiului. Simpla posibilitate de acces (cum ar fi o ușă descuiată sau o poartă deschisă într-un gard) nu implică faptul că spațiul este accesibil publicului în prezența unor indicații sau circumstanțe care sugerează contrariul (de exemplu, semne care interzic sau restricționează accesul). Sediile întreprinderilor și ale fabricilor, precum și birourile și locurile de muncă care sunt destinate a fi accesate numai de către angajații și prestatorii de servicii competenți sunt spații care nu sunt accesibile publicului. Spațiile accesibile publicului nu ar trebui să includă închisorile sau punctele de control la frontieră. Alte spații pot cuprinde atât spații accesibile publicului, cât și spații care nu sunt accesibile publicului, cum ar fi holul unei clădiri rezidențiale private, care trebuie parcurs pentru a avea acces la un cabinet medical, sau un aeroport. Spațiile online nu sunt nici ele vizate, deoarece nu sunt spații fizice. Cu toate acestea, ar trebui să se stabilească de la caz la caz dacă un anumit spațiu este accesibil publicului, având în vedere particularitățile situației individuale în cauză.

- (20) Pentru a obține beneficii cât mai mari de pe urma sistemelor de IA, protejând în același timp drepturile fundamentale, sănătatea și siguranța, și pentru a permite controlul democratic, alfabetizarea în domeniul IA ar trebui să le ofere furnizorilor, implementatorilor și persoanelor afectate noțiunile necesare pentru a lua decizii în cunoștință de cauză cu privire la sistemele de IA. Aceste noțiuni pot varia în funcție de contextul relevant și pot include înțelegerea aplicării corecte a elementelor tehnice în faza de dezvoltare a sistemului de IA, măsurile care trebuie aplicate în timpul utilizării sale, modalitățile adecvate de interpretare a rezultatelor sistemului de IA și, în cazul persoanelor afectate, cunoștințele necesare pentru a înțelege impactul pe care îl vor avea asupra lor deciziile luate cu ajutorul IA. În contextul aplicării prezentului regulament, alfabetizarea în domeniul IA ar trebui să ofere tuturor actorilor relevanți din lanțul valoric al IA informațiile necesare pentru a asigura conformitatea adecvată și aplicarea corectă a regulamentului. În plus, punerea în aplicare pe scară largă a măsurilor de alfabetizare în domeniul IA și introducerea unor acțiuni subsecvente adecvate ar putea contribui la îmbunătățirea condițiilor de muncă și, în cele din urmă, ar putea susține consolidarea unei IA de încredere și inovarea în acest domeniu în Uniune. Consiliul european pentru inteligența artificială (denumit în continuare „Consiliul IA”) ar trebui să sprijine Comisia pentru a promova instrumente de alfabetizare în domeniul IA, sensibilizarea publicului și înțelegerea beneficiilor, a riscurilor, a garanțiilor, a drepturilor și a obligațiilor care decurg din utilizarea sistemelor de IA. În cooperare cu părțile interesate relevante, Comisia și statele membre ar trebui să faciliteze elaborarea unor coduri de conduită voluntare pentru a promova alfabetizarea în domeniul IA în rândul persoanelor care se ocupă de dezvoltarea, exploatarea și utilizarea IA.

- (21) Pentru a asigura condiții de concurență echitabile și o protecție eficace a drepturilor și libertăților persoanelor fizice în întreaga Uniune, normele stabilite prin prezentul regulament ar trebui să se aplice în mod nediscriminatoriu furnizorilor de sisteme de IA, indiferent dacă sunt stabiliți în Uniune sau într-o țară terță, precum și implementatorilor de sisteme de IA stabiliți în Uniune.
- (22) Având în vedere natura lor digitală, anumite sisteme de IA ar trebui să intre în domeniul de aplicare al prezentului regulament chiar și atunci când nu sunt introduse pe piață, nu sunt puse în funcțiune și nu sunt utilizate în Uniune. Acesta este cazul, de exemplu, al unui operator stabilit în Uniune care contractează anumite servicii unui operator stabilit într-o țară terță în legătură cu o activitate care urmează să fie desfășurată de un sistem de IA care s-ar califica drept prezentând un grad ridicat de risc. În aceste circumstanțe, sistemul de IA utilizat de operator într-o țară terță ar putea prelucra date colectate în Uniune și transferate din Uniune în mod legal și ar putea furniza operatorului contractant din Uniune rezultatele produse de sistemul de IA respectiv ca urmare a prelucrării respective, fără ca sistemul de IA să fie introdus pe piață, pus în funcțiune sau utilizat în Uniune. Pentru a preveni eludarea prezentului regulament și pentru a asigura o protecție eficace a persoanelor fizice situate în Uniune, prezentul regulament ar trebui să se aplice, de asemenea, furnizorilor și implementatorilor de sisteme de IA care sunt stabiliți într-o țară terță, în măsura în care rezultatele produse de sistemele respective sunt destinate a fi utilizate în Uniune.

Cu toate acestea, pentru a ține seama de acordurile existente și de nevoile speciale de cooperare viitoare cu partenerii străini cu care se fac schimburi de informații și probe, prezentul regulament nu ar trebui să se aplice autorităților publice ale unei țări terțe și organizațiilor internaționale atunci când acestea acționează în cadrul acordurilor internaționale sau de cooperare încheiate la nivelul Uniunii sau la nivel național pentru cooperarea în materie de aplicare a legii și cooperarea judiciară cu Uniunea sau cu statele membre, cu condiția ca țara terță sau organizația internațională relevantă să ofere garanții adecvate în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor. După caz, acest lucru s-ar putea aplica activităților desfășurate de entitățile cărora țările terțe le-au încredințat îndeplinirea unor sarcini specifice în sprijinul unei astfel de cooperări judiciare și în materie de aplicare a legii. Cadrele de cooperare sau acordurile sus-menționate au fost încheiate bilateral între statele membre și țări terțe sau între Uniunea Europeană, Europol sau alte agenții ale Uniunii, pe de o parte, și țări terțe sau organizații internaționale, pe de altă parte. Autoritățile competente cu supravegherea autorităților de aplicare a legii și a autorităților judiciare în temeiul prezentului regulament ar trebui să evalueze dacă respectivele cadre de cooperare sau acorduri internaționale includ garanții adecvate în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor. Autoritățile naționale destinate și instituțiile, organele, oficiile și agențiile Uniunii care utilizează astfel de rezultate în Uniune rămân responsabile pentru asigurarea faptului că utilizarea lor respectă dreptul Uniunii. La revizuirea acordurilor internaționale respective sau la încheierea unor acorduri noi în viitor, părțile contractante ar trebui să depună toate eforturile pentru a alinia acordurile respective la cerințele prezentului regulament.

- (23) Prezentul regulament ar trebui să se aplice, de asemenea, instituțiilor, organelor, oficiilor și agențiilor Uniunii atunci când acestea acționează în calitate de furnizor sau implementator al unui sistem de IA.

- (24) În cazul și în măsura în care sistemele de IA sunt introduse pe piață, puse în funcțiune sau utilizate cu sau fără modificarea lor în scopuri militare, de apărare sau de securitate națională, sistemele respective ar trebui să fie excluse din domeniul de aplicare al prezentului regulament, indiferent de tipul de entitate care desfășoară activitățile respective, de exemplu dacă este o entitate publică sau privată. În ceea ce privește scopurile militare și de apărare, o astfel de excludere este justificată atât de articolul 4 alineatul (2) din TUE, cât și de particularitățile politicii de apărare a statelor membre și ale politicii de apărare comune a Uniunii, care intră sub incidența titlului V capitolul 2 din TUE; acestea fac obiectul dreptului internațional public, care este, prin urmare, cadrul juridic mai adecvat pentru reglementarea sistemelor de IA în contextul utilizării forței letale și a altor sisteme de IA în contextul activităților militare și de apărare. În ceea ce privește obiectivele de securitate națională, excluderea este justificată atât de faptul că securitatea națională rămâne responsabilitatea exclusivă a statelor membre în conformitate cu articolul 4 alineatul (2) din TUE, cât și de natura specifică și de nevoile operaționale ale activităților de securitate națională și de normele naționale specifice aplicabile activităților respective. Însă, în cazul în care un sistem de IA dezvoltat, introdus pe piață, pus în funcțiune sau utilizat în scopuri militare, de apărare sau de securitate națională este utilizat, temporar sau permanent, în afara acestui cadru în alte scopuri, de exemplu în scopuri civile sau umanitare, de aplicare a legii sau de securitate publică, un astfel de sistem ar intra în domeniul de aplicare al prezentului regulament. În acest caz, entitatea care utilizează sistemul de IA în alte scopuri decât cele militare, de apărare sau de securitate națională ar trebui să asigure conformitatea sistemului de IA cu prezentul regulament, cu excepția cazului în care sistemul respectă deja prezentul regulament. Sistemele de IA introduse pe piață sau puse în funcțiune pentru un scop care face obiectul excluderii, și anume în scop militar, de apărare sau de securitate națională, și pentru unul sau mai multe scopuri care nu fac obiectul excluderii, de exemplu în scopuri civile sau de aplicare a legii, intră în domeniul de aplicare al prezentului regulament, iar furnizorii sistemelor respective ar trebui să asigure conformitatea cu prezentul regulament. În aceste cazuri, faptul că un sistem de IA poate intra în domeniul de aplicare al prezentului regulament nu ar trebui să afecteze posibilitatea ca entitățile care desfășoară activități de securitate națională, de apărare și militare, indiferent de tipul de entitate care desfășoară activitățile respective, să utilizeze sisteme de IA în scopuri de securitate națională, militare și de apărare, utilizare care este exclusă din domeniul de aplicare al prezentului regulament. Un sistem de IA introdus pe piață în scopuri civile sau de aplicare a legii și care este utilizat cu sau fără modificări în scopuri militare, de apărare sau de securitate națională nu ar trebui să intre în domeniul de aplicare al prezentului regulament, indiferent de tipul de entitate care desfășoară activitățile respective.

- (25) Prezentul regulament ar trebui să sprijine inovarea, ar trebui să respecte libertatea științei și nu ar trebui să submineze activitatea de cercetare și dezvoltare. Prin urmare, este necesar să se excludă din domeniul său de aplicare sistemele și modelele de IA dezvoltate și puse în funcțiune în mod specific în scopul unic al cercetării și dezvoltării științifice. În plus, este necesar să se asigure că prezentul regulament nu afectează într-un alt mod activitatea de cercetare și dezvoltare științifică privind sistemele sau modelele de IA înainte de a fi introduse pe piață sau puse în funcțiune. În ceea ce privește activitatea de cercetare, testare și dezvoltare orientată spre produse aferentă sistemelor sau modelelor de IA, dispozițiile prezentului regulament nu ar trebui, de asemenea, să se aplice înainte ca aceste sisteme și modele să fie puse în funcțiune sau introduse pe piață. Această excludere nu aduce atingere obligației de a respecta prezentul regulament în cazul în care un sistem de IA aflat sub incidența prezentului regulament este introdus pe piață sau pus în funcțiune ca urmare a unei astfel de activități de cercetare și dezvoltare, și nici aplicării dispozițiilor privind spațiile de testare în materie de reglementare în domeniul IA și testarea în condiții reale. În plus, fără a aduce atingere excluderii sistemelor de IA dezvoltate și puse în funcțiune în mod specific în scopul unic al cercetării și dezvoltării științifice, orice alt sistem de IA care poate fi utilizat pentru desfășurarea oricărei activități de cercetare și dezvoltare ar trebui să facă în continuare obiectul dispozițiilor prezentului regulament. În orice caz, toate activitățile de cercetare și dezvoltare ar trebui să se desfășoare în conformitate cu standardele etice și profesionale recunoscute pentru cercetarea științifică, precum și în conformitate cu dreptul aplicabil al Uniunii.

- (26) Pentru a introduce un set proporțional și eficace de norme obligatorii pentru sistemele de IA, ar trebui să fie urmată o abordare bazată pe riscuri clar definită. Această abordare ar trebui să adapteze tipul și conținutul unor astfel de norme la intensitatea și amploarea riscurilor pe care le pot genera sistemele de IA. Prin urmare, este necesar să se interzică anumite practici în domeniul IA care sunt inacceptabile, să se stabilească cerințe pentru sistemele de IA cu grad ridicat de risc și obligații pentru operatorii relevanți și să se stabilească obligații în materie de transparență pentru anumite sisteme de IA.
- (27) Deși abordarea bazată pe riscuri reprezintă temelia pentru un set proporțional și eficace de norme obligatorii, este important să se reamintească Orientările în materie de etică pentru o IA fiabilă din 2019, elaborate de Grupul independent de experți la nivel înalt privind IA numit de Comisie. În orientările respective, grupul de experți a elaborat șapte principii etice fără caracter obligatoriu pentru IA, care sunt menite să contribuie la asigurarea faptului că IA este de încredere și că este solidă din punct de vedere etic. Cele șapte principii sunt: implicarea și supravegherea umană; robustețea tehnică și siguranța; respectarea vieții private și guvernanta datelor; transparența; diversitatea, nediscriminarea și echitatea; bunăstarea socială și de mediu și asumarea răspunderii. Fără a aduce atingere cerințelor obligatorii din punct de vedere juridic prevăzute în prezentul regulament și în orice alt act legislativ aplicabil al Uniunii, aceste orientări contribuie la conceperea unei IA coerente, de încredere și centrate pe factorul uman, în conformitate cu carta și cu valorile pe care se întemeiază Uniunea. Potrivit orientărilor Grupului de experți la nivel înalt privind IA, implicarea și supravegherea umană înseamnă că sistemele de IA sunt dezvoltate și utilizate ca un instrument ce servește oamenilor, respectă demnitatea umană și autonomia personală și funcționează într-un mod care poate fi controlat și supravegheat în mod corespunzător de către oameni.

Robustețea tehnică și siguranța înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod care asigură robustețea în caz de probleme și reziliența la încercările de a modifica utilizarea sau performanța sistemului de IA în vederea permiterii utilizării ilegale de către terți și care reduce la minimum prejudiciile neintenționate. Respectarea vieții private și guvernanța datelor înseamnă că sistemele de IA sunt dezvoltate și utilizate în conformitate cu normele privind protecția vieții private și a datelor și că, în același timp, se prelucrează date care respectă standarde ridicate de calitate și de integritate. Transparența înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod care permite trasabilitatea și explicabilitatea adecvate, aducând totodată la cunoștința oamenilor faptul că interacționează sau comunică cu un sistem de IA și informând în mod corespunzător implementatorii cu privire la capacitățile și limitele respectivului sistem de IA și persoanele afectate cu privire la drepturile lor. Diversitatea, nediscriminarea și echitatea înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod care presupune implicarea a diverși actori și promovează accesul egal, egalitatea de gen și diversitatea culturală, evitând totodată efectele discriminatorii și prejudecățile inechitabile interzise prin dreptul Uniunii sau dreptul intern. Bunăstarea socială și de mediu înseamnă că sistemele de IA sunt dezvoltate și utilizate într-un mod durabil, care respectă mediul și care aduce beneficii tuturor ființelor umane, monitorizându-se și evaluându-se totodată efectele pe termen lung asupra persoanelor, a societății și a democrației. Aplicarea acestor principii ar trebui să fie transpusă, atunci când este posibil, în conceperea și utilizarea modelelor de IA. În orice caz, aceste principii ar trebui să servească drept bază pentru elaborarea codurilor de conduită în temeiul prezentului regulament. Toate părțile interesate, inclusiv industria, mediul academic, societatea civilă și organizațiile de standardizare, sunt încurajate să ia în considerare, după caz, principiile etice pentru dezvoltarea de bune practici și standarde voluntare.

- (28) Pe lângă numeroasele utilizări benefice ale IA, aceasta poate fi utilizată și în mod abuziv și poate oferi instrumente noi și puternice pentru practici de manipulare, exploatare și control social. Astfel de practici sunt deosebit de nocive și abuzive și ar trebui să fie interzise deoarece contravin valorilor Uniunii privind respectarea demnității umane, a libertății, a egalității, a democrației și a statului de drept, precum și a drepturilor fundamentale consacrate în cartă, inclusiv dreptul la nediscriminare, la protecția datelor și la viața privată și drepturile copilului.

- (29) Tehnicile de manipulare bazate pe IA pot fi utilizate pentru a convinge anumite persoane să manifeste comportamente nedorite sau pentru a le înșela, împingându-le să ia decizii într-un mod care le subminează și le afectează autonomia, capacitatea decizională și libera alegere. Introducerea pe piață, punerea în funcțiune sau utilizarea anumitor sisteme de IA având drept obiectiv sau drept efect denaturarea semnificativă a comportamentului uman, caz în care este probabil să se producă prejudicii semnificative, mai ales cu efecte negative suficient de importante asupra sănătății fizice sau psihologice ori a intereselor financiare, sunt deosebit de periculoase și, prin urmare, ar trebui să fie interzise. Astfel de sisteme de IA implementează componente subliminale, cum ar fi stimuli audio, sub formă de imagini sau video, pe care persoanele nu le pot percepe întrucât stimulii respectivi depășesc percepția umană, sau alte tehnici manipulative sau înșelătoare care subminează sau afectează autonomia, capacitatea decizională sau libera alegere ale unei persoane în astfel de moduri încât oamenii nu sunt conștienți de astfel de tehnici sau, chiar dacă sunt conștienți de acestea, tot pot fi înșelați sau sunt incapabili să le controleze sau să li se opună. Acest lucru ar putea fi facilitat, de exemplu, de interfețele mașină-creier sau de realitatea virtuală, deoarece acestea permit un nivel mai ridicat de control asupra stimulilor prezentați persoanelor, în măsura în care acești stimuli pot denatura semnificativ comportamentul persoanelor într-un mod deosebit de dăunător. În plus, sistemele de IA pot exploata și în alte moduri vulnerabilitățile unei persoane sau ale unui anumit grup de persoane din cauza vârstei sau a dizabilității acestora în sensul Directivei (UE) 2019/882 a Parlamentului European și a Consiliului¹⁶ sau din cauza unei situații sociale sau economice specifice care este susceptibilă să sporească vulnerabilitatea la exploatare a persoanelor respective, cum ar fi persoanele care trăiesc în sărăcie extremă sau care aparțin minorităților etnice sau religioase.

¹⁶ Directiva (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor (JO L 151, 7.6.2019, p. 70).

Astfel de sisteme de IA pot fi introduse pe piață, puse în funcțiune sau utilizate având drept obiectiv sau drept efect denaturarea semnificativă a comportamentului unei persoane, într-un mod care cauzează sau este susceptibil în mod rezonabil să cauzeze prejudicii semnificative persoanei respective sau grupului respectiv ori unei alte persoane sau altor grupuri de persoane, inclusiv prejudicii care se pot acumula în timp, și, prin urmare, ar trebui să fie interzise. Este posibil să nu se poată presupune că există intenția de a denatura comportamentul în cazul în care denaturarea rezultă din factori externi sistemului de IA asupra cărora furnizorul sau implementatorul nu deține controlul, și anume factori care ar putea să nu fie prevăzuți în mod rezonabil și, prin urmare, să nu poată fi atenuați de către furnizorul sau implementatorul sistemului de IA. În orice caz, nu este necesar ca furnizorul sau implementatorul să aibă intenția de a cauza un prejudiciu semnificativ, cu condiția ca un astfel de prejudiciu să rezulte din practicile de manipulare sau de exploatare bazate pe IA. Interdicțiile privind astfel de practici în domeniul IA sunt complementare dispozițiilor cuprinse în Directiva 2005/29/CE a Parlamentului European și a Consiliului¹⁷, în special faptul că practicile comerciale neloiale care conduc la prejudicii economice sau financiare pentru consumatori sunt interzise în toate circumstanțele, indiferent dacă sunt puse în aplicare prin intermediul sistemelor de IA sau în alt mod. Interdicțiile privind practicile de manipulare și exploatare prevăzute în prezentul regulament nu ar trebui să afecteze practicile legale în contextul tratamentului medical, cum ar fi tratamentul psihologic al unei boli mintale sau reabilitarea fizică, atunci când practicile respective se desfășoară în conformitate cu dreptul și cu standardele medicale aplicabile, de exemplu în ceea ce privește consimțământul explicit al persoanelor în cauză sau al reprezentanților lor legali. În plus, practicile comerciale comune și legitime, de exemplu în domeniul publicității, care respectă dreptul aplicabil nu ar trebui să fie considerate, în sine, ca reprezentând practici dăunătoare de manipulare bazate pe IA.

¹⁷ Directiva 2005/29/CE a Parlamentului European și a Consiliului din 11 mai 2005 privind practicile comerciale neloiale ale întreprinderilor de pe piața internă față de consumatori și de modificare a Directivei 84/450/CEE a Consiliului, a Directivelor 97/7/CE, 98/27/CE și 2002/65/CE ale Parlamentului European și ale Consiliului și a Regulamentului (CE) nr. 2006/2004 al Parlamentului European și al Consiliului („Directiva privind practicile comerciale neloiale”) (JO L 149, 11.6.2005, p. 22).

- (30) Sistemele de clasificare biometrică care se bazează pe datele biometrice ale persoanelor fizice, cum ar fi fața sau amprente digitale ale unei persoane, pentru a face presupuneri sau deducții cu privire la opiniile politice, apartenența la un sindicat, convingerile religioase sau filozofice, rasa, viața sexuală sau orientarea sexuală ale unei persoane ar trebui să fie interzise. Această interdicție nu ar trebui să se refere la etichetarea, filtrarea sau clasificarea legală, în funcție de datele biometrice, a seturilor de date biometrice obținute în conformitate cu dreptul Uniunii sau cu dreptul intern, cum ar fi sortarea imaginilor în funcție de culoarea părului sau de culoarea ochilor, care poate fi utilizată, de exemplu, în domeniul aplicării legii.
- (31) Sistemele de IA care permit atribuirea unui punctaj social persoanelor fizice de către actori privați sau publici pot genera rezultate discriminatorii și excluderea anumitor grupuri. Acestea pot încălca dreptul la demnitate și nediscriminare, precum și valorile egalității și justiției. Astfel de sisteme de IA evaluează sau clasifică persoanele fizice sau grupurile de persoane pe baza mai multor puncte de date legate de comportamentul lor social în contexte multiple sau de caracteristici personale sau de personalitate cunoscute, deduse sau preconizate de-a lungul anumitor perioade de timp. Punctajul social obținut din astfel de sisteme de IA poate duce la un tratament prejudiciabil sau nefavorabil al persoanelor fizice sau al unor grupuri întregi de astfel de persoane în contexte sociale care nu au legătură cu contextul în care datele au fost inițial generate sau colectate sau la un tratament prejudiciabil care este disproporționat sau nejustificat în raport cu gravitatea comportamentului lor social. Sistemele de IA care implică astfel de practici inacceptabile de atribuire a unui punctaj și care conduc la astfel de rezultate prejudiciabile sau nefavorabile ar trebui, prin urmare, să fie interzise. Această interdicție nu ar trebui să afecteze practicile legale de evaluare a persoanelor fizice care sunt realizate într-un scop specific în conformitate cu dreptul Uniunii și cu dreptul național.

- (32) Utilizarea sistemelor de IA pentru identificarea biometrică la distanță „în timp real” a persoanelor fizice în spațiile accesibile publicului în scopul aplicării legii este deosebit de intruzivă pentru drepturile și libertățile persoanelor în cauză, în măsura în care poate afecta viața privată a unei părți mari a populației, poate inspira un sentiment de supraveghere constantă și poate descuraja indirect exercitarea libertății de întrunire și a altor drepturi fundamentale. Inexactitățile tehnice ale sistemelor de IA destinate identificării biometrice la distanță a persoanelor fizice pot conduce la rezultate distorsionate de prejudecăți și pot avea efecte discriminatorii. Astfel de rezultate distorsionate și efecte discriminatorii posibile sunt deosebit de relevante în ceea ce privește vârsta, etnia, rasa, sexul sau dizabilitatea. În plus, caracterul imediat al impactului și posibilitățile limitate de a efectua verificări sau corecții suplimentare în ceea ce privește utilizarea unor astfel de sisteme care funcționează în timp real implică riscuri sporite pentru drepturile și libertățile persoanelor vizate în contextul activităților de aplicare a legii sau impactate de acestea.

- (33) Prin urmare, utilizarea sistemelor respective în scopul aplicării legii ar trebui să fie interzisă, cu excepția situațiilor enumerate în mod exhaustiv și definite în mod precis în care utilizarea este strict necesară pentru un interes public substanțial, a cărui importanță este superioară riscurilor. Situațiile respective implică căutarea anumitor victime ale unor infracțiuni, inclusiv persoane dispărute, anumite amenințări la adresa vieții sau a siguranței fizice a persoanelor fizice sau privind un atac terorist și localizarea sau identificarea autorilor infracțiunilor enumerate într-o anexă la prezentul regulament sau a persoanelor suspectate de acestea, în cazul în care infracțiunile respective se pedepsesc în statul membru în cauză cu o pedeapsă sau o măsură de siguranță privativă de libertate pentru o perioadă maximă de cel puțin patru ani și astfel cum sunt definite în dreptul intern al statului membru respectiv. Un astfel de prag pentru pedeapsa sau măsura de siguranță privativă de libertate în conformitate cu dreptul intern contribuie la asigurarea faptului că infracțiunea ar trebui să fie suficient de gravă pentru a justifica eventual utilizarea sistemelor de identificare biometrică la distanță „în timp real”. În plus, lista infracțiunilor prevăzută în anexa la prezentul regulament se bazează pe cele 32 de infracțiuni enumerate în Decizia-cadru 2002/584/JAI a Consiliului¹⁸, ținând seama de faptul că unele infracțiuni sunt, în practică, susceptibile să fie mai relevante decât altele, în sensul că recurgerea la identificarea biometrică la distanță „în timp real” ar putea, în mod previzibil, fi necesară și proporțională în grade foarte diferite pentru urmărirea practică a localizării sau a identificării unui autor al diferitelor infracțiuni enumerate sau a unei persoane suspectate de acestea, și având în vedere diferențele probabile în ceea ce privește gravitatea, probabilitatea și amploarea prejudiciului sau posibilele consecințe negative.

¹⁸ Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

O amenințare iminentă la adresa vieții sau a siguranței fizice a unor persoane fizice ar putea rezulta și dintr-o perturbare gravă a infrastructurii critice, astfel cum este definită la articolul 2 punctul 4 din Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului¹⁹, în cazul în care perturbarea sau distrugerea unei astfel de infrastructuri critice ar genera o amenințare iminentă la adresa vieții sau a siguranței fizice a unei persoane, inclusiv prin afectarea gravă a aprovizionării cu produse de bază a populației sau a exercitării funcțiilor de bază ale statului. În plus, prezentul regulament ar trebui să mențină capacitatea autorităților de aplicare a legii, de control la frontiere, de imigrație sau de azil de a efectua controale de identitate în prezența persoanei vizate, în conformitate cu condițiile prevăzute în dreptul Uniunii și în cel intern pentru astfel de controale. În special, autoritățile de aplicare a legii, de control la frontiere, de imigrație sau de azil ar trebui să poată utiliza sistemele de informații, în conformitate cu dreptul Uniunii sau cu cel intern, pentru a identifica persoane care, în cursul unui control de identitate, fie refuză să fie identificate, fie sunt incapabile să își declare sau să își dovedească identitatea, fără ca autoritățile în cauză să fie obligate prin prezentul regulament să obțină o autorizație prealabilă. Ar putea fi vorba, de exemplu, de o persoană implicată într-o infracțiune care fie nu dorește, fie, din cauza unui accident sau a unei afecțiuni medicale, nu poate să își divulge identitatea autorităților de aplicare a legii.

¹⁹ Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului (JO L 333, 27.12.2022, p. 164).

- (34) Pentru a se asigura că sistemele respective sunt utilizate în mod responsabil și proporțional, este de asemenea important să se stabilească faptul că, în fiecare dintre aceste situații enumerate în mod exhaustiv și precis definite, ar trebui să fie luate în considerare anumite elemente, în special în ceea ce privește natura situației care a stat la baza cererii și consecințele utilizării asupra drepturilor și libertăților tuturor persoanelor vizate, precum și garanțiile și condițiile prevăzute pentru utilizare. În plus, ar trebui să se recurgă la utilizarea sistemelor de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul aplicării legii numai pentru a confirma identitatea persoanei vizate în mod specific și această utilizare ar trebui să se limiteze la ceea ce este strict necesar din punct de vedere al perioadei de timp, precum și al sferei de aplicare geografică și personală, având în vedere în special dovezile sau indicațiile privind amenințările, victimele sau autorul infracțiunii. Utilizarea sistemului de identificare biometrică la distanță în timp real în spațiile accesibile publicului ar trebui să fie autorizată numai dacă autoritatea relevantă de aplicare a legii a finalizat o evaluare a impactului asupra drepturilor fundamentale și, cu excepția cazului în care se prevede altfel în prezentul regulament, a înregistrat sistemul în baza de date prevăzută în prezentul regulament. Baza de date de referință a persoanelor ar trebui să fie adecvată pentru fiecare caz de utilizare în fiecare dintre situațiile menționate mai sus.

(35) Fiecare utilizare a unui sistem de identificare biometrică la distanță „în timp real” în spațiile accesibile publicului în scopul aplicării legii ar trebui să facă obiectul unei autorizări exprese și specifice de către o autoritate judiciară sau o autoritate administrativă independentă a unui stat membru a cărei decizie este obligatorie. O astfel de autorizație ar trebui, în principiu, să fie obținută înainte de utilizarea sistemului de IA în vederea identificării uneia sau mai multor persoane. Ar trebui să fie permise excepții de la această regulă în situații justificate în mod corespunzător din motive de urgență, și anume în situațiile în care necesitatea de a utiliza sistemele în cauză este de natură să facă imposibilă în mod efectiv și obiectiv obținerea unei autorizații înainte de începerea utilizării sistemului de IA. În astfel de situații de urgență, utilizarea sistemului de IA ar trebui să fie limitată la ceea ce este minim și absolut necesar și ar trebui să facă obiectul unor garanții și condiții adecvate, astfel cum sunt stabilite în dreptul intern și specificate de către însăși autoritatea de aplicare a legii în contextul fiecărui caz individual de utilizare urgentă. În plus, în astfel de situații, autoritatea de aplicare a legii ar trebui să solicite o astfel de autorizație și să furnizeze în același timp motivele pentru care nu a fost în măsură să o solicite mai devreme, fără întârzieri nejustificate și cel târziu în termen de 24 de ore. În cazul în care solicitarea unei astfel de autorizații este respinsă, utilizarea sistemelor de identificare biometrică în timp real legate de autorizația respectivă ar trebui să înceteze cu efect imediat și toate datele legate de utilizarea respectivă ar trebui să fie înlăturate și șterse. Aceste date includ datele de intrare dobândite direct de un sistem de IA în cursul utilizării unui astfel de sistem, precum și rezultatele și produsele obținute în cadrul utilizării legate de autorizația respectivă, dar nu ar trebui să includă datele de intrare dobândite în mod legal în conformitate cu un alt act legislativ al Uniunii sau național. În orice caz, nicio decizie care produce un efect juridic negativ asupra unei persoane nu ar trebui să fie luată exclusiv pe baza unui produs al sistemului de identificare biometrică la distanță.

- (36) Pentru a-și îndeplini sarcinile în conformitate cu cerințele prevăzute în prezentul regulament, precum și în normele naționale, autoritatea relevantă de supraveghere a pieței și autoritatea națională pentru protecția datelor ar trebui să fie notificate cu privire la fiecare utilizare a sistemului de identificare biometrică în timp real. Autoritățile de supraveghere a pieței și autoritățile naționale pentru protecția datelor care au fost notificate ar trebui să prezinte Comisiei un raport anual privind utilizarea sistemelor de identificare biometrică în timp real.
- (37) În plus, este oportun să se prevadă, în cadrul exhaustiv stabilit de prezentul regulament, că o astfel de utilizare pe teritoriul unui stat membru în conformitate cu prezentul regulament ar trebui să fie posibilă numai în cazul și în măsura în care statul membru respectiv a decis să prevadă în mod expres posibilitatea de a autoriza o astfel de utilizare în normele sale detaliate de drept intern. În consecință, în temeiul prezentului regulament, statele membre au în continuare libertatea de a nu prevedea o astfel de posibilitate sau de a prevedea o astfel de posibilitate numai în ceea ce privește unele dintre obiectivele care pot justifica utilizarea autorizată identificate în prezentul regulament. Astfel de norme naționale ar trebui să fie notificate Comisiei în termen de 30 de zile de la adoptare.

- (38) Utilizarea sistemelor de IA pentru identificarea biometrică la distanță în timp real a persoanelor fizice în spațiile accesibile publicului în scopul aplicării legii implică în mod necesar prelucrarea de date biometrice. Normele din prezentul regulament care interzic, sub rezerva anumitor excepții, o astfel de utilizare, care se întemeiază pe articolul 16 din TFUE, ar trebui să se aplice ca *lex specialis* în ceea ce privește normele privind prelucrarea datelor biometrice prevăzute la articolul 10 din Directiva (UE) 2016/680, reglementând astfel în mod exhaustiv această utilizare și prelucrarea datelor biometrice implicate. Prin urmare, o astfel de utilizare și prelucrare ar trebui să fie posibile numai în măsura în care sunt compatibile cu cadrul stabilit de prezentul regulament, fără a exista, în afara cadrului respectiv, posibilitatea ca autoritățile competente, atunci când acționează în scopul aplicării legii, să utilizeze astfel de sisteme și să prelucreze astfel de date în legătură cu utilizarea respectivă din motivele enumerate la articolul 10 din Directiva (UE) 2016/680. În acest context, prezentul regulament nu este menit să ofere temeiul juridic pentru prelucrarea datelor cu caracter personal în baza articolului 8 din Directiva (UE) 2016/680. Cu toate acestea, utilizarea sistemelor de identificare biometrică la distanță în timp real în spații accesibile publicului în alte scopuri decât cele de aplicare a legii, inclusiv de către autoritățile competente, nu ar trebui să facă obiectul cadrului specific privind o astfel de utilizare în scopul aplicării legii stabilit de prezentul regulament. Prin urmare, o astfel de utilizare în alte scopuri decât aplicarea legii nu ar trebui să facă obiectul solicitării unei autorizații în temeiul prezentului regulament și al normelor de drept intern detaliate aplicabile prin care autorizația respectivă poate produce efecte.

- (39) Orice prelucrare de date biometrice și alte date cu caracter personal implicate în utilizarea sistemelor de IA pentru identificarea biometrică, alta decât în legătură cu utilizarea sistemelor de identificare biometrică la distanță în timp real în spații accesibile publicului în scopul aplicării legii, astfel cum este reglementată de prezentul regulament, ar trebui să respecte în continuare toate cerințele care decurg din articolul 10 din Directiva (UE) 2016/680. În ceea ce privește alte scopuri decât aplicarea legii, articolul 9 alineatul (1) din Regulamentul (UE) 2016/679 și articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725 interzic prelucrarea de date biometrice, sub rezerva unor excepții limitate prevăzute la articolele respective. În vederea aplicării articolului 9 alineatul (1) din Regulamentul (UE) 2016/679, utilizarea identificării biometrice la distanță în alte scopuri decât aplicarea legii a făcut deja obiectul unor decizii de interzicere luate de autoritățile naționale pentru protecția datelor.

- (40) În conformitate cu articolul 6a din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Irlandei nu îi revin obligații în temeiul normelor prevăzute la articolul 5 alineatul (1) primul paragraf litera (g) în măsura în care se aplică utilizării sistemelor de clasificare biometrică pentru activități în domeniul cooperării polițienești și al cooperării judiciare în materie penală, la articolul 5 alineatul (1) primul paragraf litera (d) în măsura în care se aplică utilizării sistemelor de IA care intră sub incidența dispoziției respective, la articolul 5 alineatul (1) primul paragraf litera (h) și alineatele (2)-(6) și la articolul 26 alineatul (10) din prezentul regulament adoptate în temeiul articolului 16 din TFUE, referitoare la prelucrarea datelor cu caracter personal de către statele membre atunci când exercită activități care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE, în cazurile în care Irlandei nu îi revin obligații în temeiul normelor privind formele de cooperare judiciară în materie penală sau de cooperare polițienească care necesită respectarea dispozițiilor stabilite în temeiul articolului 16 din TFUE.

- (41) În conformitate cu articolele 2 și 2a din Protocolul nr. 22 privind poziția Danemarcei, anexat la TUE și la TFUE, Danemarcei nu îi revin obligații în temeiul normelor prevăzute la articolul 5 alineatul (1) primul paragraf litera (g) în măsura în care se aplică utilizării sistemelor de clasificare biometrică pentru activități în domeniul cooperării polițienești și al cooperării judiciare în materie penală, la articolul 5 alineatul (1) primul paragraf litera (d) în măsura în care se aplică utilizării sistemelor de IA care intră sub incidența dispoziției respective, la articolul 5 alineatul (1) primul paragraf litera (h) și alineatele (2)-(6) și la articolul 26 alineatul (10) din prezentul regulament adoptate în temeiul articolului 16 din TFUE, referitoare la prelucrarea datelor cu caracter personal de către statele membre atunci când exercită activități care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE și Danemarca nu face obiectul aplicării normelor respective.

- (42) În conformitate cu prezumția de nevinovăție, persoanele fizice din Uniune ar trebui să fie întotdeauna judecate în funcție de comportamentul lor real. Persoanele fizice nu ar trebui să fie niciodată judecate în funcție de comportamentul preconizat de IA exclusiv pe baza creării profilurilor lor, a trăsăturilor lor de personalitate sau a unor caracteristici precum cetățenia, locul nașterii, locul de reședință, numărul de copii, nivelul datoriilor sau tipul de autoturism, dacă nu există o suspiciune rezonabilă, bazată pe fapte obiective verificabile, că persoana respectivă este implicată într-o activitate infracțională și dacă nu se face o evaluare în acest sens de către un om. Prin urmare, ar trebui să fie interzise evaluările riscurilor efectuate în legătură cu persoane fizice pentru a evalua probabilitatea ca acestea să comită infracțiuni sau pentru a anticipa producerea unei infracțiuni reale sau potențiale exclusiv pe baza creării profilurilor acestor persoane sau a evaluării trăsăturilor lor de personalitate și a caracteristicilor lor. În orice caz, această interdicție nu privește și nici nu afectează analiza de risc care nu se bazează pe crearea de profiluri ale persoanelor sau pe trăsăturile de personalitate și caracteristicile persoanelor, cum ar fi sistemele de IA care utilizează analiza de risc pentru a evalua probabilitatea de fraudă financiară din partea întreprinderilor pe baza unor tranzacții suspecte sau instrumentele analitice de risc utilizate pentru a prevedea probabilitatea localizării de către autoritățile vamale a stupefiantelor sau a mărfurilor ilicite, de exemplu pe baza rutelor de trafic cunoscute.
- (43) Introducerea pe piață, punerea în funcțiune în scopul specific respectiv și utilizarea sistemelor de IA care creează sau extind baze de date de recunoaștere facială prin extragerea fără scop precis de imagini faciale de pe internet sau din înregistrări TVCI ar trebui să fie interzise, deoarece această practică amplifică sentimentul de supraveghere în masă și poate duce la încălcări grave ale drepturilor fundamentale, inclusiv ale dreptului la viață privată.

- (44) Există preocupări serioase cu privire la baza științifică a sistemelor de IA care vizează identificarea sau deducerea emoțiilor, în special deoarece exprimarea emoțiilor variază considerabil de la o cultură la alta și de la o situație la alta și chiar la nivelul unei singure persoane. Printre principalele deficiențe ale unor astfel de sisteme se numără fiabilitatea limitată, lipsa specificității și posibilitățile limitate de generalizare. Prin urmare, sistemele de IA care identifică sau deduc emoțiile sau intențiile persoanelor fizice pe baza datelor lor biometrice pot genera rezultate discriminatorii și pot fi intruzive pentru drepturile și libertățile persoanelor în cauză. Având în vedere dezechilibrul de putere în contextul muncii sau al educației, combinat cu caracterul intruziv al acestor sisteme, ele ar putea conduce la un tratament prejudiciabil sau nefavorabil al anumitor persoane fizice sau al unor grupuri întregi de astfel de persoane. Prin urmare, ar trebui să fie interzise introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA destinate a fi utilizate pentru a detecta starea emoțională a persoanelor în situații legate de locul de muncă și de educație. Această interdicție nu ar trebui să se aplice sistemelor de IA introduse pe piață strict din motive medicale sau de siguranță, cum ar fi sistemele destinate utilizării în scop terapeutic.
- (45) Practicile interzise de dreptul Uniunii, inclusiv dreptul privind protecția datelor, dreptul privind nediscriminarea, dreptul privind protecția consumatorilor și dreptul concurenței, nu ar trebui să fie afectate de prezentul regulament.

- (46) Sistemele de IA cu grad ridicat de risc ar trebui să fie introduse pe piața Uniunii, puse în funcțiune sau utilizate numai dacă respectă anumite cerințe obligatorii. Cerințele respective ar trebui să asigure faptul că sistemele de IA cu grad ridicat de risc disponibile în Uniune sau ale căror rezultate sunt utilizate în alt mod în Uniune nu prezintă riscuri inacceptabile pentru interesele publice importante ale Uniunii, astfel cum sunt recunoscute și protejate de dreptul Uniunii. Pe baza noului cadru legislativ, astfel cum s-a clarificat în Comunicarea Comisiei intitulată „Ghidul albastru» din 2022 referitor la punerea în aplicare a normelor UE privind produsele”²⁰, regula generală este că cel puțin un act juridic din legislația de armonizare a Uniunii, cum ar fi Regulamentele (UE) 2017/745²¹ și (UE) 2017/746²² ale Parlamentului European și ale Consiliului sau Directiva 2006/42/CE a Parlamentului European și a Consiliului²³, poate fi aplicabil unui singur produs, deoarece punerea la dispoziție sau punerea în funcțiune poate avea loc numai atunci când produsul respectă întreaga legislație de armonizare a Uniunii aplicabilă. Pentru a se asigura coerența și a se evita sarcinile administrative sau costurile inutile, furnizorii unui produs care conține unul sau mai multe sisteme de IA cu grad ridicat de risc, cărora li se aplică cerințele prezentului regulament și ale legislației de armonizare a Uniunii astfel cum este conținută într-o anexă la prezentul regulament, ar trebui să fie flexibili în ceea ce privește deciziile operaționale cu privire la modul optim de asigurare a conformității unui produs care conține unul sau mai multe sisteme de IA cu toate cerințele aplicabile din respectiva legislație de armonizare a Uniunii. Sistemele de IA identificate ca prezentând un grad ridicat de risc ar trebui să se limiteze la cele care au un impact negativ semnificativ asupra sănătății, siguranței și drepturilor fundamentale ale persoanelor din Uniune, iar o astfel de limitare ar trebui să reducă la minimum orice eventuală restricționare a comerțului internațional.

²⁰ JO C 247, 29.6.2022, p. 1.

²¹ Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1).

²² Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic in vitro și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

²³ Directiva 2006/42/CE a Parlamentului European și a Consiliului din 17 mai 2006 privind echipamentele tehnice și de modificare a Directivei 95/16/CE (JO L 157, 9.6.2006, p. 24).

- (47) Sistemele de IA ar putea avea un impact negativ asupra sănătății și siguranței persoanelor, în special atunci când funcționează drept componente de siguranță ale produselor. În concordanță cu obiectivele legislației de armonizare a Uniunii de a facilita libera circulație a produselor pe piața internă și de a asigura că numai produsele sigure și conforme în toate privințele ajung pe piață, este important ca riscurile în materie de siguranță care pot fi generate de un produs în ansamblu din cauza componentelor sale digitale, inclusiv a sistemelor de IA, să fie prevenite și atenuate în mod corespunzător. De exemplu, roboții din ce în ce mai autonomi, fie în contextul producției, fie în contextul asistenței și îngrijirii personale, ar trebui să fie în măsură să își desfășoare activitatea și să își îndeplinească funcțiile în condiții de siguranță în medii complexe. În mod similar, în sectorul sănătății, unde mizele privind viața și sănătatea sunt deosebit de ridicate, sistemele de diagnosticare din ce în ce mai sofisticate și sistemele care sprijină deciziile umane ar trebui să fie fiabile și exacte.

- (48) Amploarea impactului negativ al sistemului de IA asupra drepturilor fundamentale protejate de cartă este deosebit de relevantă atunci când un sistem de IA este clasificat ca prezentând un grad ridicat de risc. Printre aceste drepturi se numără dreptul la demnitate umană, respectarea vieții private și de familie, protecția datelor cu caracter personal, libertatea de exprimare și de informare, libertatea de întrunire și de asociere, precum, dreptul la nediscriminare, dreptul la educație, protecția consumatorilor, drepturile lucrătorilor, drepturile persoanelor cu dizabilități, egalitatea de gen, drepturile de proprietate intelectuală, dreptul la o cale de atac eficientă și la un proces echitabil, dreptul la apărare și prezumția de nevinovăție și dreptul la o bună administrare. Pe lângă aceste drepturi, este important să se sublinieze faptul că copiii au drepturi specifice, astfel cum sunt consacrate la articolul 24 din cartă și în Convenția Organizației Națiunilor Unite cu privire la drepturile copilului, detaliată în Comentariul general nr. 25 la aceasta privind mediul digital, ambele impunând luarea în considerare a vulnerabilităților copiilor și asigurarea protecției și îngrijirii necesare pentru bunăstarea lor. Dreptul fundamental la un nivel ridicat de protecție a mediului consacrat în cartă și pus în aplicare în politicile Uniunii ar trebui, de asemenea, să fie luat în considerare atunci când se evaluează gravitatea prejudiciului pe care îl poate cauza un sistem de IA, inclusiv în ceea ce privește sănătatea și siguranța persoanelor.

- (49) În ceea ce privește sistemele de IA cu grad ridicat de risc care sunt componente de siguranță ale produselor sau sistemelor sau care sunt ele însele produse sau sisteme care intră în domeniul de aplicare al Regulamentului (CE) nr. 300/2008 al Parlamentului European și al Consiliului²⁴, al Regulamentului (UE) nr. 167/2013 al Parlamentului European și al Consiliului²⁵, al Regulamentului (UE) nr. 168/2013 al Parlamentului European și al Consiliului²⁶, al Directivei 2014/90/UE a Parlamentului European și a Consiliului²⁷, al Directivei (UE) 2016/797 a Parlamentului European și a Consiliului²⁸, al Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului²⁹,

²⁴ Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72).

²⁵ Regulamentul (UE) nr. 167/2013 al Parlamentului European și al Consiliului din 5 februarie 2013 privind omologarea și supravegherea pieței pentru vehiculele agricole și forestiere (JO L 60, 2.3.2013, p. 1).

²⁶ Regulamentul (UE) nr. 168/2013 al Parlamentului European și al Consiliului din 15 ianuarie 2013 privind omologarea și supravegherea pieței pentru vehiculele cu două sau trei roți și pentru cvadricicluri (JO L 60, 2.3.2013, p. 52).

²⁷ Directiva 2014/90/UE a Parlamentului European și a Consiliului din 23 iulie 2014 privind echipamentele maritime și de abrogare a Directivei 96/98/CE a Consiliului (JO L 257, 28.8.2014, p. 146).

²⁸ Directiva (UE) 2016/797 a Parlamentului European și a Consiliului din 11 mai 2016 privind interoperabilitatea sistemului feroviar în Uniunea Europeană (JO L 138, 26.5.2016, p. 44).

²⁹ Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului din 30 mai 2018 privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE (JO L 151, 14.6.2018, p. 1).

al Regulamentului (UE) 2018/1139 al Parlamentului European și al Consiliului³⁰ și al Regulamentului (UE) 2019/2144 al Parlamentului European și al Consiliului³¹, este oportun să se modifice respectivele acte legislative pentru a se asigura luarea în considerare de către Comisie, pe baza specificităților tehnice și de reglementare ale fiecărui sector și fără a afecta mecanismele și autoritățile existente de guvernare, de evaluare a conformității și de aplicare a legislației instituite în acestea, a cerințelor obligatorii pentru sistemele de IA cu grad ridicat de risc prevăzute în prezentul regulament atunci când adoptă orice act delegat sau de punere în aplicare relevant pe baza respectivelor acte legislative.

³⁰ Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1).

³¹ Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului din 27 noiembrie 2019 privind cerințele pentru omologarea de tip a autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate unor astfel de vehicule, în ceea ce privește siguranța generală a acestora și protecția ocupanților vehiculului și a utilizatorilor vulnerabili ai drumurilor, de modificare a Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului și de abrogare a Regulamentelor (CE) nr. 78/2009, (CE) nr. 79/2009 și (CE) nr. 661/2009 ale Parlamentului European și ale Consiliului și a Regulamentelor (CE) nr. 631/2009, (UE) nr. 406/2010, (UE) nr. 672/2010, (UE) nr. 1003/2010, (UE) nr. 1005/2010, (UE) nr. 1008/2010, (UE) nr. 1009/2010, (UE) nr. 19/2011, (UE) nr. 109/2011, (UE) nr. 458/2011, (UE) nr. 65/2012, (UE) nr. 130/2012, (UE) nr. 347/2012, (UE) nr. 351/2012, (UE) nr. 1230/2012 și (UE) 2015/166 ale Comisiei (JO L 325, 16.12.2019, p. 1).

- (50) În ceea ce privește sistemele de IA care sunt componente de siguranță ale produselor sau care sunt ele însele produse care intră în domeniul de aplicare al anumitor acte legislative de armonizare ale Uniunii enumerate într-o anexă la prezentul regulament, este oportun să fie clasificate ca prezentând un grad ridicat de risc în temeiul prezentului regulament în cazul în care produsul respectiv este supus procedurii de evaluare a conformității efectuate de un organism terț de evaluare a conformității în temeiul respectivelor acte legislative de armonizare relevante ale Uniunii. În special, astfel de produse sunt echipamentele tehnice, jucăriile, ascensoarele, echipamentele și sistemele de protecție destinate utilizării în atmosfere potențial explozive, echipamentele radio, echipamentele sub presiune, echipamentele pentru ambarcațiuni de agrement, instalațiile pe cablu, aparatele consumatoare de combustibili gazoși, dispozitivele medicale, dispozitivele medicale pentru diagnostic in vitro, cele din industria auto și aeronautică.
- (51) Clasificarea unui sistem de IA ca prezentând un grad ridicat de risc în temeiul prezentului regulament nu ar trebui să însemne neapărat că produsul a cărui componentă de siguranță este sistemul de IA sau că sistemul de IA în sine ca produs este considerat ca prezentând un grad ridicat de risc în conformitate cu criteriile stabilite în actele legislative de armonizare relevante ale Uniunii care se aplică produsului. Acesta este, în special, cazul Regulamentelor (UE) 2017/745 și (UE) 2017/746, care prevăd o evaluare a conformității de către un terț pentru produsele cu grad mediu de risc și cu grad ridicat de risc.

- (52) În ceea ce privește sistemele de IA autonome, și anume alte sisteme de IA cu grad ridicat de risc decât cele care sunt componente de siguranță ale unor produse sau care sunt ele însele produse, este oportun să fie clasificate ca prezentând un grad ridicat de risc dacă, având în vedere scopul lor preconizat, prezintă un risc ridicat de a aduce prejudicii sănătății și siguranței sau drepturilor fundamentale ale persoanelor, ținându-se seama atât de gravitatea posibilelor prejudicii, cât și de probabilitatea producerii acestora, și dacă sunt utilizate într-o serie de domenii predefinite în mod specific precizate în prezentul regulament. Identificarea sistemelor respective se bazează pe aceeași metodologie și pe aceleași criterii avute în vedere pentru eventuale modificări viitoare ale listei de sisteme de IA cu grad ridicat de risc, modificări pe care Comisia ar trebui să fie împuternicită să le adopte, prin intermediul unor acte delegate, pentru a ține seama de ritmul rapid al dezvoltării tehnologice și de eventualele modificări în utilizarea sistemelor de IA.

- (53) De asemenea, este important să se clarifice faptul că pot exista cazuri specifice în care sistemele de IA menționate în domeniile predefinite specificate în prezentul regulament nu conduc la un risc semnificativ de a aduce prejudicii intereselor juridice protejate în cadrul domeniilor respective, deoarece nu influențează în mod semnificativ procesul decizional sau nu aduc prejudicii substanțiale intereselor respective. În sensul prezentului regulament, un sistem de IA care nu influențează în mod semnificativ rezultatul procesului decizional ar trebui să fie înțeles ca fiind un sistem de IA care nu are un impact asupra substanței și, prin urmare, nici asupra rezultatului procesului decizional, indiferent dacă este uman sau automatizat. Un sistem de IA care nu influențează în mod semnificativ rezultatul procesului decizional ar putea include situații în care sunt îndeplinite una sau mai multe dintre condițiile prezentate în continuare. Prima condiție ar trebui să fie aceea ca sistemul de IA să fie destinat să îndeplinească o sarcină procedurală restrânsă, de exemplu un sistem de IA care transformă date nestructurate în date structurate, un sistem de IA care clasifică pe categorii documentele primite sau un sistem de IA care este utilizat pentru a detecta duplicatele dintr-un număr mare de candidaturi. Aceste sarcini au un caracter atât de restrâns și de limitat încât prezintă doar riscuri reduse, riscuri care nu cresc prin utilizarea unui sistem de IA într-un context enumerat ca utilizare cu grad ridicat de risc într-o anexă la prezentul regulament. A doua condiție ar trebui să fie ca sarcina îndeplinită de sistemul de IA să fie menită să îmbunătățească rezultatul unei activități umane finalizate anterior care poate fi relevantă în sensul utilizărilor cu grad ridicat de risc enumerate într-o anexă la prezentul regulament. Având în vedere aceste caracteristici, sistemul de IA adaugă doar un nivel suplimentar unei activități umane, prezentând în consecință un risc redus. Această condiție s-ar aplica, de exemplu, sistemelor de IA care sunt menite să îmbunătățească limbajul utilizat în documente redactate anterior, de exemplu în ceea ce privește tonul profesional, stilul academic de limbaj sau alinierea textului la mesajele specifice unei anumite mărci. A treia condiție ar trebui să fie aceea ca sistemul de IA să fie destinat să detecteze modelele decizionale sau devierile de la modele decizionale anterioare.

Riscul ar fi redus deoarece utilizarea sistemului de IA este ulterioară unei evaluări finalizate anterior de către un om, pe care nu este destinată să o înlocuiască sau să o influențeze fără o revizuire adecvată de către un om. Printre aceste sisteme de IA se numără, de exemplu, cele care, având în vedere un anumit model de notare folosit de un cadru didactic, pot fi utilizate pentru a verifica *ex post* dacă respectivul cadru didactic s-a abătut de la modelul de notare în cauză și pentru a semnala astfel eventuale inconsecvențe sau anomalii. A patra condiție ar trebui să fie aceea ca sistemul de IA să fie destinat să îndeplinească o sarcină care este doar pregătitoare pentru o evaluare relevantă pentru scopurile sistemelor de IA enumerate într-o anexă la prezentul regulament, făcând astfel ca posibilul impact al rezultatelor sistemului să prezinte un risc foarte scăzut pentru evaluarea ulterioară bazată pe ele. Această condiție se referă, printre altele, la soluțiile inteligente de gestionare a fișierelor, care includ diverse funcții, cum ar fi indexarea, căutarea, prelucrarea textelor și a vorbirii sau corelarea datelor cu alte surse de date, ori la sistemele de IA utilizate pentru traducerea documentelor inițiale. În orice caz, ar trebui să se considere că sistemele de IA utilizate în situații cu grad ridicat de risc enumerate într-o anexă la prezentul regulament prezintă riscuri semnificative de prejudicii la adresa sănătății, siguranței sau drepturilor fundamentale dacă implică crearea de profiluri în sensul articolului 4 punctul 4 din Regulamentul (UE) 2016/679 sau al articolului 3 punctul 4 din Directiva (UE) 2016/680 sau al articolului 3 punctul 5 din Regulamentul (UE) 2018/1725. Pentru a asigura trasabilitatea și transparența, un furnizor care consideră pe baza condițiilor menționate mai sus că un sistem de IA nu prezintă un grad ridicat de risc ar trebui să întocmească documentația pentru evaluare înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune și ar trebui să furnizeze respectiva documentație autorităților naționale competente, la cerere. Furnizorul ar trebui să fie obligat să înregistreze sistemul de IA în baza de date a UE instituită în temeiul prezentului regulament. Pentru a oferi îndrumare suplimentară în vederea punerii în practică a condițiilor în care sistemele de IA enumerate într-o anexă la prezentul regulament nu prezintă, în mod excepțional, un grad ridicat de risc, Comisia ar trebui, după consultarea Consiliului IA, să furnizeze orientări care să detalieze respectiva punere în practică, completate de o listă cuprinzătoare de exemple practice de cazuri de utilizare a sistemelor de IA cu grad ridicat de risc și cazuri de utilizare fără grad ridicat de risc.

- (54) Întrucât datele biometrice constituie o categorie specială de date cu caracter personal, este oportun ca mai multe cazuri de utilizare critică a sistemelor biometrice să fie clasificate ca prezentând un grad ridicat de risc, în măsura în care utilizarea acestora este permisă în temeiul dreptului Uniunii și al dreptului intern relevant. Inexactitățile tehnice ale sistemelor de IA destinate identificării biometrice la distanță a persoanelor fizice pot conduce la rezultate distorsionate de prejudecăți și pot avea efecte discriminatorii. Riscul unor astfel de rezultate distorsionate de prejudecăți și efecte discriminatorii este deosebit de relevant în ceea ce privește vârsta, etnia, rasa, sexul sau dizabilitățile. Prin urmare, sistemele de identificare biometrică la distanță ar trebui să fie clasificate ca prezentând un grad ridicat de risc, având în vedere riscurile pe care le implică. Nu se încadrează în această clasificare sistemele de IA destinate a fi utilizate pentru verificarea biometrică, inclusiv pentru autentificare, al cărei unic scop este de a confirma că o anumită persoană fizică este cine susține că este și de a confirma identitatea unei persoane fizice cu unicul scop de a-i permite accesul la un serviciu, deblocarea unui dispozitiv sau accesul securizat într-o incintă. În plus, ar trebui să fie clasificate ca prezentând un grad ridicat de risc sistemele de IA destinate a fi utilizate pentru clasificarea biometrică în funcție de attribute sau caracteristici sensibile protejate în temeiul articolului 9 alineatul (1) din Regulamentul (UE) 2016/679 pe baza datelor biometrice, în măsura în care nu sunt interzise în temeiul prezentului regulament, și sistemele de recunoaștere a emoțiilor care nu sunt interzise în temeiul prezentului regulament. Sistemele biometrice destinate a fi utilizate exclusiv în scopul aplicării măsurilor de securitate cibernetică și de protecție a datelor cu caracter personal nu ar trebui să fie considerate sisteme de IA cu grad ridicat de risc.

- (55) În ceea ce privește gestionarea și exploatarea infrastructurii critice, este oportun să se clasifice ca prezentând un grad ridicat de risc sistemele de IA destinate utilizării drept componente de siguranță în cadrul gestionării și exploatării infrastructurilor digitale critice enumerate la punctul 8 din anexa la Directiva (UE) 2022/2557, a traficului rutier și a aprovizionării cu apă, gaz, încălzire și energie electrică, deoarece defectarea lor sau funcționarea lor defectuoasă poate pune în pericol viața și sănătatea persoanelor la scară largă și poate conduce la perturbări semnificative ale desfășurării obișnuite a activităților sociale și economice. Componentele de siguranță ale infrastructurii critice, inclusiv ale infrastructurii digitale critice, sunt sisteme utilizate pentru a proteja în mod direct integritatea fizică a infrastructurii critice sau sănătatea și siguranța persoanelor și a bunurilor, dar care nu sunt necesare pentru funcționarea sistemului. Defectarea sau funcționarea defectuoasă a unor astfel de componente ar putea conduce în mod direct la riscuri pentru integritatea fizică a infrastructurii critice și, prin urmare, la riscuri pentru sănătatea și siguranța persoanelor și a bunurilor. Componentele destinate a fi utilizate exclusiv în scopuri de securitate cibernetică nu ar trebui să se califice drept componente de siguranță. Printre exemplele de componente de siguranță ale unei astfel de infrastructuri critice se numără sistemele de monitorizare a presiunii apei sau sistemele de control al alarmei de incendiu în centrele de cloud computing.

- (56) Implementarea sistemelor de IA în educație este importantă pentru a promova educația și formarea digitală de înaltă calitate și pentru a permite tuturor cursanților și cadrelor didactice să dobândească și să partajeze aptitudinile și competențele digitale necesare, inclusiv educația în domeniul mass-mediei și gândirea critică, pentru a participa activ la economie, în societate și la procesele democratice. Cu toate acestea, sistemele de IA utilizate în educație sau în formarea profesională, în special pentru stabilirea accesului sau a admiterii, pentru repartizarea persoanelor în instituții sau programe educaționale și de formare profesională la toate nivelurile, pentru evaluarea rezultatelor învățării unei persoane, pentru evaluarea nivelului adecvat de instruire al unei persoane, pentru influențarea semnificativă a nivelului de educație și formare pe care îl vor primi sau îl vor putea accesa persoanele sau pentru monitorizarea și detectarea comportamentului interzis al elevilor și studenților în timpul testelor, ar trebui să fie clasificate drept sisteme de IA cu grad ridicat de risc, deoarece pot determina parcursul educațional și profesional din viața unei persoane și, prin urmare, pot afecta capacitatea acesteia de a-și asigura mijloace de subzistență. Atunci când sunt concepute și utilizate în mod necorespunzător, astfel de sisteme pot fi deosebit de intruzive și pot încălca dreptul la educație și formare, precum și dreptul de a nu fi discriminat și pot perpetua tipare istorice de discriminare, de exemplu împotriva femeilor, a anumitor grupe de vârstă, a persoanelor cu dizabilități sau a persoanelor de anumite origini rasiale ori etnice sau cu o anumită orientare sexuală.

- (57) De asemenea, sistemele de IA utilizate în domeniul ocupării forței de muncă, al gestionării lucrătorilor și al accesului la activități independente, în special pentru recrutarea și selectarea persoanelor, pentru luarea deciziilor care afectează condițiile relației legate de muncă, pentru promovarea și încetarea relațiilor contractuale legate de muncă, pentru alocarea sarcinilor pe baza comportamentului individual sau a trăsăturilor sau caracteristicilor personale, precum și pentru monitorizarea sau evaluarea persoanelor aflate în relații contractuale legate de muncă, ar trebui să fie clasificate ca prezentând un grad ridicat de risc, deoarece aceste sisteme pot avea un impact semnificativ asupra viitoarelor perspective de carieră, asupra mijloacelor de subzistență ale acestor persoane și asupra drepturilor lucrătorilor. Relațiile contractuale relevante legate de muncă ar trebui să implice într-un mod semnificativ angajații și persoanele care prestează servicii prin intermediul platformelor, astfel cum se menționează în Programul de lucru al Comisiei pentru 2021. Pe tot parcursul procesului de recrutare, precum și în evaluarea, promovarea sau menținerea persoanelor în relații contractuale legate de muncă, astfel de sisteme pot perpetua tipare istorice de discriminare, de exemplu împotriva femeilor, a anumitor grupe de vârstă, a persoanelor cu dizabilități sau a persoanelor de anumite origini rasiale ori etnice sau cu o anumită orientare sexuală. Sistemele de IA utilizate pentru a monitoriza performanța și comportamentul acestor persoane pot, de asemenea, să le submineze drepturile fundamentale la protecția datelor și la viața privată.

- (58) Un alt domeniu în care utilizarea sistemelor de IA merită o atenție deosebită este accesul și posibilitatea de a beneficia de anumite prestații și servicii publice și private esențiale, necesare pentru ca oamenii să participe pe deplin în societate sau să își îmbunătățească nivelul de trai. În special, persoanele fizice care solicită sau primesc prestații și servicii esențiale de asistență publică din partea autorităților publice, și anume servicii de îngrijiri de sănătate, prestații de asigurări sociale, servicii sociale care oferă protecție în cazuri precum maternitatea, boala, accidentele de muncă, dependența, bătrânețea, pierderea locului de muncă, precum și asistență socială și legată de locuințe, sunt de regulă dependente de aceste prestații și servicii și se află într-o poziție vulnerabilă în raport cu autoritățile responsabile. În cazul în care sistemele de IA sunt utilizate pentru a stabili dacă astfel de prestații și servicii ar trebui să fie acordate, refuzate, reduse, revocate sau recuperate de autorități, inclusiv dacă beneficiarii au dreptul legitim la astfel de prestații sau servicii, sistemele respective pot avea un impact semnificativ asupra mijloacelor de subzistență ale persoanelor și le pot încălca drepturile fundamentale, cum ar fi dreptul la protecție socială, la nediscriminare, la demnitatea umană sau la o cale de atac efectivă și, prin urmare, ar trebui să fie clasificate ca prezentând un grad ridicat de risc. Cu toate acestea, prezentul regulament nu ar trebui să împiedice dezvoltarea și utilizarea unor abordări inovatoare în administrația publică, care ar putea beneficia de o utilizare mai largă a sistemelor de IA conforme și sigure, cu condiția ca aceste sisteme să nu implice un risc ridicat pentru persoanele fizice și juridice.

În plus, sistemele de IA utilizate pentru a evalua punctajul de credit sau bonitatea persoanelor fizice ar trebui să fie clasificate ca sisteme de IA cu grad ridicat de risc, întrucât acestea determină accesul persoanelor respective la resurse financiare sau la servicii esențiale, cum ar fi locuințe, electricitate și telecomunicații. Sistemele de IA utilizate în aceste scopuri pot duce la discriminare între persoane sau între grupuri și pot perpetua tipare istorice de discriminare, de exemplu pe criterii de origine rasială sau etnică, sex, dizabilitate, vârstă sau orientare sexuală, sau pot crea noi forme de impact discriminatoriu. Cu toate acestea, sistemele de IA prevăzute de dreptul Uniunii în scopul detectării fraudelor în furnizarea de servicii financiare și în scopuri prudențiale pentru a calcula cerințele de capital ale instituțiilor de credit și ale întreprinderilor de asigurări nu ar trebui să fie considerate ca prezentând un grad ridicat de risc în temeiul prezentului regulament. În plus, sistemele de IA destinate a fi utilizate pentru evaluarea riscurilor și stabilirea prețurilor pentru asigurarea de sănătate și de viață în cazul persoanelor fizice pot avea, de asemenea, un impact semnificativ asupra mijloacelor de subzistență ale persoanelor și, dacă nu sunt concepute, dezvoltate și utilizate în mod corespunzător, pot încălca drepturile lor fundamentale și pot avea consecințe grave pentru viața și sănătatea oamenilor, cum ar fi excluziunea financiară și discriminarea. În cele din urmă, sistemele de IA utilizate pentru evaluarea și clasificarea apelurilor de urgență ale persoanelor fizice sau pentru distribuirea sau stabilirea priorităților în distribuirea serviciilor de primă intervenție de urgență, inclusiv de către poliție, pompieri și asistența medicală, precum și în cadrul sistemelor de triaj medical de urgență al pacienților, ar trebui de asemenea să fie clasificate ca prezentând un grad ridicat de risc, deoarece iau decizii în situații foarte critice pentru viața și sănătatea persoanelor și pentru bunurile acestora.

- (59) Având în vedere rolul și responsabilitatea lor, acțiunile întreprinse de autoritățile de aplicare a legii care implică anumite utilizări ale sistemelor de IA sunt caracterizate de un grad semnificativ de dezechilibru de putere și pot duce la supravegherea, arestarea sau privarea de libertate a unei persoane fizice, precum și la alte efecte negative asupra drepturilor fundamentale garantate în cartă. În special, în cazul în care nu este alimentat cu date de înaltă calitate, nu îndeplinește cerințe adecvate de performanță, acuratețe sau robustețe sau nu este proiectat și testat în mod corespunzător înainte de a fi introdus pe piață sau pus în funcțiune în alt mod, sistemul de IA poate selecta persoanele într-un mod discriminatoriu sau, la un nivel mai general, în mod incorect ori injust. În plus, exercitarea unor drepturi procedurale fundamentale importante, cum ar fi dreptul la o cale de atac efectivă și la un proces echitabil, precum și dreptul la apărare și prezumția de nevinovăție, ar putea fi împiedicată, în special în cazul în care astfel de sisteme de IA nu sunt suficient de transparente, explicabile și documentate. Prin urmare, este oportun să fie clasificate ca prezentând un grad ridicat de risc, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii și al dreptului intern relevant, o serie de sisteme de IA destinate a fi utilizate în contextul aplicării legii, în care acuratețea, fiabilitatea și transparența sunt deosebit de importante pentru a evita efectele negative, pentru a păstra încrederea publicului și pentru a asigura asumarea răspunderii și reparații efective.

Având în vedere natura activităților și riscurile aferente, aceste sisteme de IA cu grad ridicat de risc ar trebui să includă, în special, sistemele de IA destinate a fi utilizate de autoritățile de aplicare a legii sau în numele acestora sau de instituțiile, organele, oficiile sau agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru a evalua riscul ca o persoană fizică să devină victimă a infracțiunilor, ca poligrafe și instrumente similare pentru evaluarea fiabilității probelor în cursul investigării sau urmăririi penale a infracțiunilor și, în măsura în care nu se interzice în temeiul prezentului regulament, pentru a evalua riscul ca o persoană fizică să comită o infracțiune sau o recidivă, nu numai pe baza creării de profiluri ale persoanelor fizice, a evaluării trăsăturilor de personalitate și a caracteristicilor lor sau a comportamentului infracțional anterior al persoanelor fizice sau al grupurilor, precum și pentru a crea profiluri în cursul depistării, investigării sau urmăririi penale a infracțiunilor. Sistemele de IA destinate în mod specific utilizării în proceduri administrative de către autoritățile fiscale și vamale, precum și de către unitățile de informații financiare care efectuează sarcini administrative prin care analizează informații în temeiul dreptului Uniunii privind combaterea spălării banilor, nu ar trebui să fie clasificate ca sisteme de IA cu grad ridicat de risc utilizate de autoritățile de aplicare a legii în scopul prevenirii, depistării, investigării și urmăririi penale a infracțiunilor. Utilizarea instrumentelor de IA de către autoritățile de aplicare a legii și de alte autorități relevante nu ar trebui să devină un factor de inegalitate sau de excluziune. Impactul utilizării instrumentelor de IA asupra drepturilor la apărare ale suspectilor nu ar trebui să fie ignorat, în special dificultatea de a obține informații semnificative cu privire la funcționarea acestor sisteme și, în consecință, dificultatea de a contesta rezultatele acestora în instanță, în special de către persoanele fizice care fac obiectul investigării.

(60) Sistemele de IA utilizate în domeniile migrației, azilului și gestionării controlului la frontiere afectează persoane care se află adesea într-o poziție deosebit de vulnerabilă și care depind de rezultatul acțiunilor autorităților publice competente. Acuratețea, caracterul nediscriminatoriu și transparența sistemelor de IA utilizate în aceste contexte sunt, prin urmare, deosebit de importante pentru a garanta respectarea drepturilor fundamentale ale persoanelor afectate, în special a drepturilor acestora la liberă circulație, nediscriminare, protecția vieții private și a datelor cu caracter personal, protecție internațională și bună administrare. Prin urmare, este oportun să fie clasificate ca prezentând un grad ridicat de risc, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii și al dreptului intern relevant, sistemele de IA destinate a fi utilizate de către autoritățile publice competente ori în numele acestora sau de către instituțiile, organele, oficiile sau agențiile Uniunii care au atribuții în domeniile migrației, azilului și gestionării controlului la frontiere ca poligrafe și instrumente similare, pentru a evalua anumite riscuri prezentate de persoanele fizice care intră pe teritoriul unui stat membru sau care solicită viză sau azil, pentru a acorda asistență autorităților publice competente în ceea ce privește examinarea, inclusiv evaluarea conexă a fiabilității probelor, a cererilor de azil, de vize și de permise de ședere și a plângerilor aferente cu privire la obiectivul de stabilire a eligibilității persoanelor fizice care solicită un statut, în scopul detectării, al recunoașterii sau al identificării persoanelor fizice în contextul migrației, al azilului și al gestionării controlului la frontiere, cu excepția verificării documentelor de călătorie.

Sistemele de IA din domeniul migrației, azilului și gestionării controlului la frontiere reglementate de prezentul regulament ar trebui să respecte cerințele procedurale relevante stabilite de Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului³², de Directiva 2013/32/UE a Parlamentului European și a Consiliului³³ și de alte dispoziții relevante din dreptul Uniunii. Statele membre sau instituțiile, organele, oficiile și agențiile Uniunii nu ar trebui în niciun caz să utilizeze sistemele de IA în domeniul migrației, azilului și gestionării controlului la frontiere ca mijloc de eludare a obligațiilor lor internaționale în temeiul Convenției ONU privind statutul refugiaților întocmită la Geneva la 28 iulie 1951, astfel cum a fost modificată prin Protocolul din 31 ianuarie 1967. De asemenea, respectivele sisteme de IA nu ar trebui să fie utilizate pentru a încălca în vreun fel principiul nereturnării sau pentru a refuza căi legale sigure și eficace de intrare pe teritoriul Uniunii, inclusiv dreptul la protecție internațională.

³² Regulamentul (CE) nr. 810/2009 al Parlamentului European și al Consiliului din 13 iulie 2009 privind instituirea unui Cod comunitar de vize (Codul de vize) (JO L 243, 15.9.2009, p. 1).

³³ Directiva 2013/32/UE a Parlamentului European și a Consiliului din 26 iunie 2013 privind procedurile comune de acordare și retragere a protecției internaționale (JO L 180, 29.6.2013, p. 60).

- (61) Anumite sisteme de IA destinate administrării justiției și proceselor democratice ar trebui să fie clasificate ca prezentând un grad ridicat de risc, având în vedere impactul potențial semnificativ al acestora asupra democrației, statului de drept și libertăților individuale, precum și asupra dreptului la o cale de atac efectivă și la un proces echitabil. În special, pentru a aborda potențialele riscuri de prejudecăți, erori și opacitate, este oportun să fie calificate drept sisteme cu grad ridicat de risc sistemele de IA destinate să fie utilizate de o autoritate judiciară sau în numele acesteia pentru a ajuta autoritățile judiciare să cerceteze și să interpreteze faptele și legea și să aplice legea unui set concret de fapte. Sistemele de IA destinate a fi utilizate de organismele de soluționare alternativă a litigiilor în aceste scopuri ar trebui, de asemenea, să fie considerate ca având un grad ridicat de risc atunci când rezultatele procedurilor de soluționare alternativă a litigiilor produc efecte juridice pentru părți. Utilizarea instrumentelor de IA poate sprijini puterea de decizie a judecătorilor sau independența sistemului judiciar, dar nu ar trebui să le înlocuiască: procesul decizional final trebuie să rămână o activitate umană. Clasificarea sistemelor de IA ca prezentând un grad ridicat de risc nu ar trebui, totuși, să se extindă la sistemele de IA destinate unor activități administrative pur auxiliare care nu afectează administrarea efectivă a justiției în cazuri individuale, cum ar fi anonimizarea sau pseudonimizarea hotărârilor judecătorești, a documentelor sau a datelor, comunicarea între membrii personalului, sarcinile administrative.

- (62) Fără a aduce atingere normelor prevăzute în Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului³⁴⁺ și pentru a aborda riscurile de ingerințe externe nejustificate în dreptul de vot consacrat la articolul 39 din cartă și de efecte adverse asupra democrației și a statului de drept, sistemele de IA destinate a fi utilizate pentru a influența rezultatul unor alegeri sau al unui referendum sau comportamentul de vot al persoanelor fizice în exercitarea votului lor în cadrul alegerilor sau al referendumurilor ar trebui să fie clasificate drept sisteme de IA cu grad ridicat de risc, cu excepția sistemelor de IA la ale căror rezultate persoanele fizice nu sunt expuse în mod direct, cum ar fi instrumentele utilizate pentru organizarea, optimizarea și structurarea campaniilor politice din punct de vedere administrativ și logistic.
- (63) Faptul că un sistem de IA este clasificat ca sistem de IA cu grad ridicat de risc în temeiul prezentului regulament nu ar trebui să fie interpretat ca indicând că utilizarea sistemului este legală în temeiul altor acte ale dreptului Uniunii sau al dreptului intern compatibil cu dreptul Uniunii, cum ar fi în ceea ce privește protecția datelor cu caracter personal, utilizarea poligrafelor și a instrumentelor similare sau a altor sisteme pentru detectarea stării emoționale a persoanelor fizice. Orice astfel de utilizare ar trebui să continue să aibă loc numai în conformitate cu cerințele aplicabile care decurg din cartă, precum și din legislația secundară aplicabilă a Uniunii și din dreptul intern aplicabil. Prezentul regulament nu ar trebui să fie înțeles ca oferind temeiul juridic pentru prelucrarea datelor cu caracter personal, inclusiv a categoriilor speciale de date cu caracter personal, după caz, cu excepția cazului în care se specifică altfel în cuprinsul prezentului regulament.

³⁴ Regulamentul (UE) nr. 2024/... al Parlamentului European și al Consiliului din ... privind transparența și vizarea unui public-țintă în publicitatea politică (JO L, ..., ELI: ...).

⁺ JO: a se introduce în text numărul regulamentului din PE-CONS 90/23 [2021/0381 (COD)] și a se completa nota de subsol corespunzătoare.

- (64) Pentru atenuarea riscurilor generate de sistemele de IA cu grad ridicat de risc introduse pe piață sau puse în funcțiune și pentru a asigura un nivel înalt de credibilitate, ar trebui să se aplice anumite cerințe obligatorii în cazul sistemelor de IA cu grad ridicat de risc, ținând seama de scopul preconizat și de contextul utilizării sistemului de IA și în conformitate cu sistemul de gestionare a riscurilor care urmează să fie instituit de furnizor. Măsurile adoptate de furnizori pentru a se conforma cerințelor obligatorii din prezentul regulament ar trebui să țină seama de stadiul general recunoscut al tehnologiei în materie de IA, să fie proporționale și eficace pentru a îndeplini obiectivele prezentului regulament. Pe baza noului cadru legislativ, astfel cum s-a clarificat în Comunicarea Comisiei intitulată „«Ghidul albastru» din 2022 referitor la punerea în aplicare a normelor UE privind produsele”, regula generală este că cel puțin un act juridic din legislația de armonizare a Uniunii poate fi aplicabil unui singur produs, deoarece punerea la dispoziție sau punerea în funcțiune poate avea loc numai atunci când produsul respectă întreaga legislație de armonizare a Uniunii aplicabilă. Pericolele sistemelor de IA care fac obiectul cerințelor prezentului regulament se referă la aspecte diferite față de legislația existentă de armonizare a Uniunii și, prin urmare, cerințele prezentului regulament ar completa corpul existent al legislației de armonizare a Uniunii. De exemplu, mașinile sau dispozitivele medicale care încorporează un sistem de IA ar putea prezenta riscuri care nu sunt abordate de cerințele esențiale de sănătate și siguranță prevăzute în legislația armonizată relevantă a Uniunii, deoarece legislația sectorială respectivă nu abordează riscurile specifice sistemelor de IA.

Acest lucru necesită o aplicare simultană și complementară a diferitelor acte legislative. Pentru a se asigura coerența și a se evita sarcinile administrative și costurile inutile, furnizorii unui produs care conține unul sau mai multe sisteme de IA cu grad ridicat de risc, cărora li se aplică cerințele prezentului regulament și ale legislației de armonizare a Uniunii bazate pe noul cadru legislativ și care figurează într-o anexă la prezentul regulament, ar trebui să fie flexibili în ceea ce privește deciziile operaționale cu privire la modul optim de asigurare a conformității unui produs care conține unul sau mai multe sisteme de IA cu toate cerințele aplicabile din respectiva legislație armonizată a Uniunii. Această flexibilitate ar putea însemna, de exemplu, o decizie a furnizorului de a integra o parte a proceselor de testare și raportare necesare, informațiile și documentația impuse în temeiul prezentului regulament în documentația și în procedurile deja existente impuse în temeiul legislației de armonizare existente a Uniunii bazate pe noul cadru legislativ și care figurează într-o anexă la prezentul regulament. Acest lucru nu ar trebui să submineze în niciun fel obligația furnizorului de a respecta toate cerințele aplicabile.

- (65) Sistemul de gestionare a riscurilor ar trebui să constea într-un proces iterativ continuu care este preconizat și derulat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc. Respectivul proces ar trebui să aibă drept scop identificarea și atenuarea riscurilor relevante reprezentate de sistemele de IA pentru sănătate, siguranță și drepturile fundamentale. Sistemul de gestionare a riscurilor ar trebui să fie evaluat și actualizat periodic pentru a se asigura eficacitatea sa continuă, precum și justificarea și documentarea oricăror decizii și acțiuni semnificative luate în temeiul prezentului regulament. Acest proces ar trebui să garanteze faptul că furnizorul identifică riscurile sau efectele negative și pune în aplicare măsuri de atenuare pentru riscurile cunoscute și previzibile în mod rezonabil reprezentate de sistemele de IA pentru sănătate, siguranță și drepturile fundamentale, având în vedere scopul preconizat al acestora și utilizarea necorespunzătoare previzibilă în mod rezonabil ale acestor sisteme, inclusiv posibilele riscuri care decurg din interacțiunea dintre sistemele de IA și mediul în care funcționează. Sistemul de gestionare a riscurilor ar trebui să adopte cele mai adecvate măsuri de gestionare a riscurilor, având în vedere stadiul cel mai avansat al tehnologiei în domeniul IA. Atunci când identifică cele mai adecvate măsuri de gestionare a riscurilor, furnizorul ar trebui să documenteze și să explice alegerile făcute și, după caz, să implice experți și părți interesate externe. Atunci când identifică utilizarea necorespunzătoare previzibilă în mod rezonabil a sistemelor de IA cu grad ridicat de risc, furnizorul ar trebui să acopere utilizările sistemelor de IA în legătură cu care se poate aștepta în mod rezonabil, să rezulte dintr-un comportament uman ușor previzibil în contextul caracteristicilor specifice și al utilizării unui anumit sistem de IA, deși utilizările respective nu sunt acoperite în mod direct de scopul preconizat și nu sunt prevăzute în instrucțiunile de utilizare. Orice circumstanțe cunoscute sau previzibile legate de utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu scopul său preconizat sau în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil, care pot conduce la riscuri pentru sănătate și siguranță sau pentru drepturile fundamentale, ar trebui să fie incluse în instrucțiunile de utilizare care sunt furnizate de furnizor. Scopul este de a se asigura că implementatorul le cunoaște și le ia în considerare atunci când utilizează sistemul de IA cu grad ridicat de risc. Identificarea și punerea în aplicare a măsurilor de atenuare a riscurilor în caz de utilizare necorespunzătoare previzibilă în temeiul prezentului regulament nu ar trebui să necesite din partea furnizorului antrenare suplimentară specifică pentru sistemul de IA cu grad ridicat de risc pentru a aborda utilizarea necorespunzătoare previzibilă. Cu toate acestea, furnizorii sunt încurajați să ia în considerare astfel de măsuri suplimentare de antrenare pentru a atenua utilizările necorespunzătoare previzibile în mod rezonabil, după cum este necesar și adecvat.

- (66) Cerințele ar trebui să se aplice sistemelor de IA cu grad ridicat de risc în ceea ce privește gestionarea riscurilor, calitatea și relevanța seturilor de date utilizate, documentația tehnică și păstrarea evidențelor, transparența și furnizarea de informații către implementatori, supravegherea umană, robustețea, acuratețea și securitatea cibernetică. Aceste cerințe sunt necesare pentru a atenua în mod eficace riscurile pentru sănătate, siguranță și drepturile fundamentale. Nefiind disponibile în mod rezonabil alte măsuri mai puțin restrictive privind comerțul, respectivele restricții în calea comerțului nu sunt astfel nejustificate.

(67) Datele de înaltă calitate și accesul la date de înaltă calitate joacă un rol vital în ceea ce privește furnizarea structurii și asigurarea performanței multor sisteme de IA, în special atunci când se utilizează tehnici care implică antrenarea modelelor, pentru a se asigura că sistemul de IA cu grad ridicat de risc funcționează astfel cum s-a prevăzut și în condiții de siguranță și nu devine o sursă de discriminare, interzisă de dreptul Uniunii. Seturile de date de înaltă calitate de antrenare, de validare și de testare necesită punerea în aplicare a unor practici adecvate de guvernanță și gestionare a datelor. Seturile de date de antrenare, de validare și de testare, inclusiv etichetele, ar trebui să fie relevante, suficient de reprezentative și, pe cât posibil, fără erori și complete, având în vedere scopul preconizat al sistemului. Pentru a facilita respectarea dreptului Uniunii în materie de protecție a datelor, cum ar fi Regulamentul (UE) 2016/679, practicile de guvernanță și gestionare a datelor ar trebui să includă, în cazul datelor cu caracter personal, transparența cu privire la scopul inițial al colectării datelor. Seturile de date ar trebui să aibă, de asemenea, proprietățile statistice adecvate, inclusiv în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul de IA cu grad ridicat de risc, acordând o atenție deosebită atenuării posibilelor prejudecăți din seturile de date, care ar putea afecta sănătatea și siguranța persoanelor, ar putea avea un impact negativ asupra drepturilor fundamentale sau ar putea conduce la discriminare interzisă în temeiul dreptului Uniunii, în special în cazul în care datele de ieșire influențează datele de intrare pentru operațiunile viitoare („bucle de feedback”). Prejudecățile pot fi, de exemplu, inerente seturilor de date subiacente, mai ales când sunt utilizate date istorice, sau pot fi generate în timpul implementării în condiții reale a sistemelor.

Rezultatele produse de sistemele de IA ar putea fi influențate de aceste prejudecăți inerente care tind să crească treptat și astfel să perpetueze și să amplifice discriminarea existentă, în special pentru persoanele care aparțin anumitor grupuri vulnerabile, inclusiv grupuri rasiale sau etnice. Cerința ca seturile de date să fie, pe cât posibil, complete și fără erori nu ar trebui să afecteze utilizarea tehnicilor de protejare a vieții private în contextul dezvoltării și testării sistemelor de IA. În special, seturile de date ar trebui să țină seama, în măsura în care acest lucru este necesar având în vedere scopul lor preconizat, de particularitățile, caracteristicile sau elementele care sunt specifice cadrului geografic, contextual, comportamental sau funcțional în care este destinat să fie utilizat sistemul de IA. Cerințele legate de guvernanta datelor pot fi respectate prin recurgerea la părți terțe care oferă servicii de conformitate certificate, inclusiv verificarea guvernantei datelor, a integrității seturilor de date și a practicilor de antrenare, validare și testare a datelor, în măsura în care este asigurată respectarea cerințelor în materie de date din prezentul regulament.

- (68) Pentru dezvoltarea și evaluarea sistemelor de IA cu grad ridicat de risc, anumiți actori, cum ar fi furnizorii, organismele notificate și alte entități relevante, cum ar fi centrele europene de inovare digitală, unitățile de testare și experimentare și cercetătorii, ar trebui să poată accesa și utiliza seturi de date de înaltă calitate în domeniile de activitate ale actorilor respectivi care sunt legate de prezentul regulament. Spațiile europene comune ale datelor instituite de Comisie și facilitarea schimbului de date între întreprinderi și cu administrațiile publice în interes public vor fi esențiale pentru a oferi un acces de încredere, responsabil și nediscriminatoriu la date de înaltă calitate pentru antrenarea, validarea și testarea sistemelor de IA. De exemplu, în domeniul sănătății, spațiul european al datelor privind sănătatea va facilita accesul nediscriminatoriu la datele privind sănătatea și antrenarea algoritmilor IA cu aceste seturi de date, într-un mod care protejează viața privată, sigur, prompt, transparent și fiabil și cu o guvernanță instituțională adecvată. Autoritățile competente relevante, inclusiv cele sectoriale, care furnizează sau sprijină accesul la date pot sprijini, de asemenea, furnizarea de date de înaltă calitate pentru antrenarea, validarea și testarea sistemelor de IA.
- (69) Dreptul la viața privată și la protecția datelor cu caracter personal trebuie să fie garantat pe parcursul întregului ciclu de viață al sistemului de IA. În acest sens, principiile reducerii la minimum a datelor și protecției datelor începând cu momentul conceperii și în mod implicit, astfel cum sunt prevăzute în dreptul Uniunii privind protecția datelor, sunt aplicabile atunci când sunt prelucrate date cu caracter personal. Măsurile luate de furnizori pentru a asigura respectarea principiilor respective pot include nu numai anonimizarea și criptarea, ci și folosirea unei tehnologii care permite să se aplice algoritmi datelor și antrenarea sistemelor de IA, fără ca aceste date să fie transmise între părți și fără ca înseși datele primare sau datele structurate să fie copiate, fără a aduce atingere cerințelor privind guvernanța datelor prevăzute în prezentul regulament.

- (70) Pentru a proteja dreptul altora împotriva discriminării care ar putea rezulta din prejudecățile inerente sistemelor de IA, furnizorii ar trebui să poată să prelucreze și categorii speciale de date cu caracter personal, ca o chestiune de interes public major în înțelesul articolului 9 alineatul (2) litera (g) din Regulamentul (UE) 2016/679 și al articolului 10 alineatul (2) litera (g) din Regulamentul (UE) 2018/1725, în mod excepțional, în măsura în care este strict necesar în scopul asigurării detectării și corectării prejudecăților în legătură cu sistemele de IA cu grad ridicat de risc, sub rezerva unor garanții adecvate pentru drepturile și libertățile fundamentale ale persoanelor fizice și în urma aplicării tuturor condițiilor prevăzute în temeiul prezentului regulament în plus față de condițiile prevăzute în Regulamentele (UE) 2016/679 și (UE) 2018/1725 și în Directiva (UE) 2016/680.
- (71) Deținerea de informații ușor de înțeles cu privire la modul în care au fost dezvoltate sistemele de IA cu grad ridicat de risc și la modul în care acestea funcționează pe toată durata lor de viață este esențială pentru a permite trasabilitatea sistemelor respective, pentru a verifica conformitatea cu cerințele prevăzute în prezentul regulament, precum și pentru monitorizarea funcționării lor și pentru monitorizarea ulterioară introducerii pe piață. Acest lucru presupune păstrarea evidențelor și disponibilitatea unei documentații tehnice care să conțină informațiile necesare pentru a evalua conformitatea sistemului de IA cu cerințele relevante și a facilita monitorizarea ulterioară introducerii pe piață. Aceste informații ar trebui să includă caracteristicile generale, capabilitățile și limitările sistemului, algoritmi, datele, procesele de antrenare, testare și validare utilizate, precum și documentația privind sistemul relevant de gestionare a riscurilor și ar trebui să fie redactate într-o formă clară și cuprinzătoare. Documentația tehnică ar trebui să fie actualizată permanent și în mod adecvat pe toată durata de viață a sistemului de IA. În plus, sistemele de IA cu grad ridicat de risc ar trebui să permită din punct de vedere tehnic înregistrarea automată a evenimentelor, prin intermediul unor fișiere de jurnalizare, de-a lungul duratei de viață a sistemului.

- (72) Pentru a răspunde preocupărilor legate de opacitatea și complexitatea anumitor sisteme de IA și pentru a-i ajuta pe implementatori să își îndeplinească obligațiile care le revin în temeiul prezentului regulament, ar trebui să fie impusă transparența pentru sistemele de IA cu grad ridicat de risc înainte ca acestea să fie introduse pe piață sau puse în funcțiune. Sistemele de IA cu grad ridicat de risc ar trebui să fie proiectate astfel încât să le permită implementatorilor să înțeleagă modul în care funcționează sistemul de IA, să îi evalueze funcționalitatea și să îi înțeleagă punctele forte și limitările. Sistemele de IA cu grad ridicat de risc ar trebui să fie însoțite de informații adecvate sub formă de instrucțiuni de utilizare. Astfel de informații ar trebui să includă caracteristicile, capacitățile și limitările performanței sistemului de IA. Acestea ar acoperi informații privind posibile circumstanțe cunoscute și previzibile legate de utilizarea sistemului de IA cu grad ridicat de risc, inclusiv acțiuni ale implementatorului care pot influența comportamentul și performanța sistemului, din cauza cărora sistemul de IA poate genera riscuri pentru sănătate, siguranță și drepturile fundamentale, privind modificările care au fost prestabilite și evaluate din punctul de vedere al conformității de către furnizor și privind măsurile relevante de supraveghere umană, inclusiv măsurile de facilitare a interpretării rezultatelor sistemului de IA de către implementatori. Transparența, inclusiv instrucțiunile de utilizare însoțitoare, ar trebui să ajute implementatorii să utilizeze sistemul și să îi sprijine să ia decizii în cunoștință de cauză. Printre altele, implementatorii ar trebui să fie mai în măsură să aleagă corect sistemul pe care intenționează să îl utilizeze, având în vedere obligațiile care le sunt aplicabile, să fie informați despre utilizările preconizate și interzise și să utilizeze sistemul de IA în mod corect și adecvat. Pentru a spori lizibilitatea și accesibilitatea informațiilor incluse în instrucțiunile de utilizare, ar trebui să fie incluse, după caz, exemple ilustrative, de exemplu privind limitările și utilizările preconizate și interzise ale sistemului de IA. Furnizorii ar trebui să se asigure că toată documentația, inclusiv instrucțiunile de utilizare, conține informații semnificative, cuprinzătoare, accesibile și ușor de înțeles, ținând seama de nevoile și cunoștințele previzibile ale implementatorilor vizați. Instrucțiunile de utilizare ar trebui să fie puse la dispoziție într-o limbă ușor de înțeles de către implementatorii vizați, astfel cum se stabilește de statul membru în cauză.

- (73) Sistemele de IA cu grad ridicat de risc ar trebui să fie concepute și dezvoltate astfel încât persoanele fizice să poată supraveghea funcționarea lor și să se poată asigura că ele sunt utilizate conform destinației lor și că impactul lor este abordat pe parcursul întregului ciclu de viață al sistemului. În acest scop, furnizorul sistemului ar trebui să identifice măsuri adecvate de supraveghere umană înainte de introducerea sa pe piață sau de punerea sa în funcțiune. În special, după caz, astfel de măsuri ar trebui să garanteze că sistemul este supus unor constrângeri operaționale integrate care nu pot fi dezactivate de sistem și care sunt receptive la operatorul uman și că persoanele fizice cărora le-a fost încredințată supravegherea umană au competența, pregătirea și autoritatea necesare pentru îndeplinirea acestui rol. De asemenea, este esențial, după caz, să se asigure faptul că sistemele de IA cu grad ridicat de risc includ mecanisme de ghidare și informare a unei persoane fizice căreia i-a fost încredințată supravegherea umană pentru a lua decizii în cunoștință de cauză pentru a stabili dacă, când și cum să intervină pentru a evita consecințele negative sau riscurile sau pentru a opri sistemul dacă nu funcționează astfel cum s-a prevăzut. Având în vedere consecințele semnificative pentru persoane în cazul unei concordanțe incorecte generate de anumite sisteme de identificare biometrică, este oportun să se prevadă o cerință de supraveghere umană mai strictă pentru sistemele respective, astfel încât implementatorul să nu poată lua nicio măsură sau decizie pe baza identificării rezultate din sistem, decât dacă acest lucru a fost verificat și confirmat separat de cel puțin două persoane fizice. Aceste persoane ar putea proveni de la una sau mai multe entități și ar putea include persoana care operează sau utilizează sistemul. Această cerință nu ar trebui să reprezinte o povară inutilă sau să genereze întârzieri inutile și ar putea fi suficient ca verificările separate efectuate de diferite persoane să fie înregistrate automat în fișierele de jurnalizare generate de sistem. Având în vedere particularitățile din domeniile aplicării legii, migrației, controlului la frontiere și azilului, această cerință nu ar trebui să se aplice în cazul în care dreptul Uniunii sau dreptul intern consideră că aplicarea cerinței respective este disproporționată.

(74) Sistemele de IA cu grad ridicat de risc ar trebui să funcționeze în mod consecvent pe parcursul întregului lor ciclu de viață și să atingă un nivel adecvat de acuratețe, robustețe și securitate cibernetică, având în vedere scopul lor preconizat și în conformitate cu stadiul de avansare al tehnologiei general recunoscut. Comisia și organizațiile și părțile interesate relevante sunt încurajate să țină seama în mod corespunzător de atenuarea riscurilor și a impacturilor negative ale sistemului de IA. Nivelul preconizat al indicatorilor de performanță ar trebui să fie declarat în instrucțiunile de utilizare însoțitoare. Furnizorii sunt îndemnați să comunice aceste informații implementatorilor într-un mod clar și ușor de înțeles, fără inducere în eroare sau declarații înșelătoare. Dreptul Uniunii privind metrologia legală, inclusiv Directivele 2014/31/UE³⁵ și 2014/32/UE³⁶ ale Parlamentului European și ale Consiliului, urmărește să asigure acuratețea măsurărilor și să contribuie la transparența și echitatea tranzacțiilor comerciale. În acest context, în cooperare cu părțile interesate și organizațiile relevante, cum ar fi autoritățile din domeniul metrologiei și al etalonării, Comisia ar trebui să încurajeze, după caz, elaborarea unor valori de referință și a unor metodologii de măsurare pentru sistemele de IA. În acest sens, Comisia ar trebui să țină seama de partenerii internaționali care lucrează în domeniul metrologiei și al indicatorilor de măsurare relevanți referitori la IA și să colaboreze cu partenerii respectivi.

³⁵ Directiva 2014/31/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a aparatelor de cântărit cu funcționare neautomată (JO L 96, 29.3.2014, p. 107).

³⁶ Directiva 2014/32/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a mijloacelor de măsurare (JO L 096, 29.3.2014, p. 149).

- (75) Robustețea tehnică este o cerință esențială pentru sistemele de IA cu grad ridicat de risc. Acestea ar trebui să fie reziliente în raport cu comportamentul prejudiciabil sau altfel indezirabil, care poate rezulta din limitările din cadrul sistemelor sau al mediului în care funcționează sistemele (de exemplu, erori, defecțiuni, inconsecvențe, situații neprevăzute). Prin urmare, ar trebui să fie luate măsuri tehnice și organizatorice pentru a asigura robustețea sistemelor de IA cu grad ridicat de risc, de exemplu prin proiectarea și dezvoltarea de soluții tehnice adecvate pentru a preveni sau a reduce la minimum comportamentul prejudiciabil sau altfel indezirabil în alt mod. Soluțiile tehnice respective pot include, de exemplu, mecanisme care permit sistemului să își întrerupă funcționarea în condiții de siguranță (planuri de autoprotecție) în prezența anumitor anomalii sau atunci când funcționarea are loc în afara anumitor limite prestabilite. Incapacitatea de a asigura protecția împotriva acestor riscuri ar putea avea un impact asupra siguranței sau ar putea afecta în mod negativ drepturile fundamentale, de exemplu din cauza unor decizii eronate sau a unor rezultate greșite sau distorsionate de prejudecăți generate de sistemul de IA.
- (76) Securitatea cibernetică joacă un rol esențial în asigurarea rezilienței sistemelor de IA împotriva încercărilor de modificare a utilizării, a comportamentului, a performanței sau de compromitere a proprietăților lor de securitate de către părți terțe răuvoitoare care exploatează vulnerabilitățile sistemului. Atacurile cibernetice împotriva sistemelor de IA se pot folosi de active specifice de IA, cum ar fi seturi de date de antrenament (de exemplu, otrăvirea datelor) sau modele antrenate (de exemplu, atacuri contradictorii sau inferențe din datele membrilor – *membership inference*), sau pot exploata vulnerabilitățile activelor digitale ale sistemului de IA sau ale infrastructurii TIC subiacente. Pentru a asigura un nivel de securitate cibernetică adecvat riscurilor, furnizorii de sisteme de IA cu grad ridicat de risc ar trebui, prin urmare, să ia măsuri adecvate, cum ar fi controalele de securitate, ținând seama, după caz, și de infrastructura TIC subiacentă.

(77) Fără a aduce atingere cerințelor legate de robustețe și acuratețe prevăzute în prezentul regulament, sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale, în conformitate cu regulamentul respectiv, pot demonstra conformitatea cu cerințele de securitate cibernetică prevăzute în prezentul regulament prin îndeplinirea cerințelor esențiale de securitate cibernetică prevăzute în regulamentul respectiv. Atunci când îndeplinesc cerințele esențiale ale Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale, sistemele de IA cu grad ridicat de risc ar trebui să fie considerate conforme cu cerințele de securitate cibernetică prevăzute în prezentul regulament, în măsura în care îndeplinirea cerințelor respective este demonstrată în declarația de conformitate UE sau în părți ale acesteia emise în temeiul regulamentului respectiv. În acest scop, evaluarea riscurilor în materie de securitate cibernetică asociate unui produs cu elemente digitale clasificat drept sistem de IA cu grad ridicat de risc în conformitate cu prezentul regulament, efectuată în temeiul Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale, ar trebui să ia în considerare riscurile la adresa rezilienței cibernetică a unui sistem de IA în ceea ce privește încercările unor părți terțe neautorizate de a-i modifica utilizarea, comportamentul sau performanța, inclusiv vulnerabilitățile specifice IA, cum ar fi otrăvirea datelor sau atacurile contradictorii, precum și, după caz, riscurile la adresa drepturilor fundamentale, astfel cum se prevede în prezentul regulament.

(78) Procedura de evaluare a conformității prevăzută de prezentul regulament ar trebui să se aplice în ceea ce privește cerințele esențiale în materie de securitate cibernetică ale unui produs cu elemente digitale care intră sub incidența Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și clasificat drept sistem de IA cu grad ridicat de risc în temeiul prezentului regulament. Totuși, această regulă nu ar trebui să conducă la reducerea nivelului necesar de asigurare pentru produsele critice cu elemente digitale care intră sub incidența Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale. Prin urmare, prin derogare de la această regulă, sistemele de IA cu grad ridicat de risc care intră în domeniul de aplicare al prezentului regulament și care sunt calificate, de asemenea, drept produse importante și critice cu elemente digitale în temeiul Regulamentului Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și cărora li se aplică procedura de evaluare a conformității bazată pe control intern prevăzută într-o anexă la prezentul regulament fac obiectul dispozițiilor privind evaluarea conformității din Regulamentul Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale în ceea ce privește cerințele esențiale în materie de securitate cibernetică din regulamentul respectiv. În acest caz, pentru toate celelalte aspecte reglementate de prezentul regulament ar trebui să se aplice dispozițiile respective privind evaluarea conformității bazate pe control intern prevăzute într-o anexă la prezentul regulament. Valorificând cunoașterea și cunoștințele de specialitate din ENISA în ceea ce privește politica în materie de securitate cibernetică și sarcinile atribuite ENISA în temeiul Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului³⁷, Comisia ar trebui să coopereze cu ENISA în ceea ce privește aspectele legate de securitatea cibernetică a sistemelor de IA.

³⁷ Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

- (79) Este oportun ca o anumită persoană fizică sau juridică, definită drept furnizor, să își asume responsabilitatea pentru introducerea pe piață sau punerea în funcțiune a unui sistem de IA cu grad ridicat de risc, indiferent dacă persoana fizică sau juridică respectivă este persoana care a proiectat sau a dezvoltat sistemul.
- (80) În calitate de semnatare ale Convenției Națiunilor Unite privind drepturile persoanelor cu dizabilități, Uniunea și statele membre sunt obligate din punct de vedere juridic să protejeze persoanele cu dizabilități împotriva discriminării și să promoveze egalitatea acestora, să se asigure că persoanele cu dizabilități au acces, în condiții de egalitate cu ceilalți, la tehnologiile și sistemele informației și comunicațiilor și să garanteze respectarea vieții private a persoanelor cu dizabilități. Având în vedere importanța și utilizarea în creștere a sistemelor de IA, aplicarea principiilor proiectării universale la toate noile tehnologii și servicii ar trebui să asigure accesul deplin și egal al tuturor persoanelor potențial afectate de tehnologiile IA sau care utilizează aceste tehnologii, inclusiv al persoanelor cu dizabilități, într-un mod care să țină seama pe deplin de demnitatea și diversitatea lor inerentă. Prin urmare, este esențial ca furnizorii să asigure conformitatea deplină cu cerințele de accesibilitate, inclusiv cu Directiva (UE) 2016/2102 a Parlamentului European și a Consiliului³⁸ și cu Directiva (UE) 2019/882. Furnizorii ar trebui să asigure conformitatea cu aceste cerințe din faza de proiectare. Prin urmare, măsurile necesare ar trebui să fie integrate cât mai mult posibil în proiectarea sistemului de IA cu grad ridicat de risc.

³⁸ Directiva (UE) 2016/2102 a Parlamentului European și a Consiliului din 26 octombrie 2016 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public (JO L 327, 2.12.2016, p. 1).

- (81) Furnizorul ar trebui să instituie un sistem bine pus la punct de management al calității, să asigure realizarea procedurii necesare de evaluare a conformității, să întocmească documentația relevantă și să instituie un sistem solid de monitorizare după introducerea pe piață. Furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor obligații privind sistemele de management al calității în temeiul dreptului sectorial relevant al Uniunii ar trebui să aibă posibilitatea de a include elementele sistemului de management al calității prevăzut în prezentul regulament ca parte a sistemului existent de management al calității prevăzut în respectivul drept sectorial al Uniunii. Complementaritatea dintre prezentul regulament și dreptul sectorial existent al Uniunii ar trebui, de asemenea, să fie luată în considerare în viitoarele activități de standardizare sau orientări adoptate de Comisie. Autoritățile publice care pun în funcțiune sisteme de IA cu grad ridicat de risc pentru uzul propriu pot adopta și pune în aplicare norme privind sistemul de management al calității ca parte a sistemului de management al calității adoptat la nivel național sau regional, după caz, ținând seama de particularitățile sectorului și de competențele și organizarea autorității publice în cauză.

- (82) Pentru a permite aplicarea prezentului regulament și pentru a crea condiții de concurență echitabile pentru operatori și ținând seama de diferitele forme de punere la dispoziție a produselor digitale, este important să se asigure că, în toate circumstanțele, o persoană stabilită în Uniune poate furniza autorităților toate informațiile necesare cu privire la conformitatea unui sistem de IA. Prin urmare, înainte de a-și pune la dispoziție sistemele de IA în Uniune, furnizorii stabiliți în țări terțe ar trebui să desemneze, prin mandat scris, un reprezentant autorizat stabilit în Uniune. Respectivul reprezentant autorizat joacă un rol central în asigurarea conformității sistemelor de IA cu grad ridicat de risc introduse pe piață sau puse în funcțiune în Uniune de furnizorii respectivi care nu sunt stabiliți în Uniune și în îndeplinirea rolului de persoană de contact a acestora stabilită în Uniune.
- (83) Având în vedere natura și complexitatea lanțului valoric pentru sistemele de IA și în conformitate cu noul cadru legislativ, este esențial să se asigure securitatea juridică și să se faciliteze respectarea prezentului regulament. Prin urmare, este necesar să se clarifice rolul și obligațiile specifice ale operatorilor relevanți de-a lungul lanțului valoric respectiv, cum ar fi importatorii și distribuitorii care pot contribui la dezvoltarea sistemelor de IA. În anumite situații, operatorii respectivi ar putea acționa în mai multe roluri în același timp și, prin urmare, ar trebui să îndeplinească în mod cumulativ toate obligațiile relevante asociate rolurilor respective. De exemplu, un operator ar putea acționa în același timp ca distribuitor și ca importator.

- (84) Pentru a se asigura securitatea juridică, este necesar să se clarifice că, în anumite condiții specifice, orice distribuitor, importator, implementator sau altă parte terță ar trebui să fie considerat drept furnizor al unui sistem de IA cu grad ridicat de risc și, prin urmare, să își asume toate obligațiile relevante. Acest lucru ar fi valabil dacă partea respectivă își pune numele sau marca comercială pe un sistem de IA cu grad ridicat de risc deja introdus pe piață sau pus în funcțiune, fără a aduce atingere dispozițiilor contractuale care prevăd că obligațiile sunt alocate în alt mod. Acest lucru ar fi valabil și dacă partea respectivă aduce o modificare substanțială unui sistem de IA cu grad ridicat de risc care a fost deja introdus pe piață sau a fost deja pus în funcțiune și într-un mod în care acesta rămâne un sistem de IA cu grad ridicat de risc în conformitate cu prezentul regulament sau dacă modifică scopul preconizat al unui sistem de IA, inclusiv al unui sistem de IA de uz general, care nu a fost clasificat ca prezentând un grad ridicat de risc și care a fost deja introdus pe piață sau pus în funcțiune, într-un mod în care sistemul de IA devine un sistem de IA cu grad ridicat de risc în conformitate cu prezentul regulament. Aceste dispoziții ar trebui să se aplice fără a aduce atingere dispozițiilor mai specifice stabilite în anumite acte legislative de armonizare ale Uniunii întemeiate pe noul cadru legislativ, împreună cu care ar trebui să se aplice prezentul regulament. De exemplu, articolul 16 alineatul (2) din Regulamentul (UE) 2017/745, care stabilește că anumite modificări nu ar trebui să fie considerate modificări ale unui dispozitiv care ar putea afecta conformitatea acestuia cu cerințele aplicabile, ar trebui să se aplice în continuare sistemelor de IA cu grad ridicat de risc care sunt dispozitive medicale în sensul regulamentului respectiv.

- (85) Sistemele de IA de uz general pot fi utilizate în sine ca sisteme de IA cu grad ridicat de risc sau pot fi componente ale altor sisteme de IA cu grad ridicat de risc. Prin urmare, având în vedere natura lor specifică și pentru a asigura o partajare echitabilă a responsabilităților de-a lungul lanțului valoric al IA, furnizorii de astfel de sisteme ar trebui, indiferent dacă pot fi utilizate ca sisteme de IA cu grad ridicat de risc ca atare de alți furnizori sau drept componente ale unor sisteme de IA cu grad ridicat de risc și cu excepția cazului în care se prevede altfel în prezentul regulament, să coopereze îndeaproape cu furnizorii sistemelor de IA cu grad ridicat de risc relevante pentru a permite respectarea de către acestea a obligațiilor relevante în temeiul prezentului regulament și cu autoritățile competente instituite în temeiul prezentului regulament.
- (86) În cazul în care, în condițiile prevăzute în prezentul regulament, furnizorul care a introdus inițial sistemul de IA pe piață sau l-a pus în funcțiune nu ar mai trebui să fie considerat furnizor în sensul prezentului regulament și în cazul în care furnizorul respectiv nu a exclus în mod expres schimbarea sistemului de IA într-un sistem de IA cu grad ridicat de risc, primul furnizor ar trebui totuși să coopereze îndeaproape, să pună la dispoziție informațiile necesare și să furnizeze accesul tehnic și alte tipuri de asistență preconizate în mod rezonabil care sunt necesare pentru îndeplinirea obligațiilor prevăzute în prezentul regulament, în special în ceea ce privește respectarea cerințelor privind evaluarea conformității sistemelor de IA cu grad ridicat de risc.
- (87) În plus, în cazul în care un sistem de IA cu grad ridicat de risc care este o componentă de siguranță a unui produs care intră în domeniul de aplicare al legislației de armonizare a Uniunii întemeiate pe noul cadru legislativ nu este introdus pe piață sau pus în funcțiune independent de produs, fabricantul produsului definit în legislația respectivă ar trebui să respecte obligațiile furnizorului stabilite în prezentul regulament și ar trebui, în special, să se asigure că sistemul de IA încorporat în produsul final respectă cerințele prezentului regulament.

- (88) De-a lungul lanțului valoric al IA, numeroase părți furnizează adesea sisteme, instrumente și servicii de IA, dar și componente sau procese care sunt încorporate de furnizor în sistemul de IA, cu diferite obiective, inclusiv antrenarea modelelor, reconversia modelelor, testarea și evaluarea modelelor, integrarea în software sau alte aspecte ale dezvoltării de modele. Respectivul părți au un rol important în lanțul valoric față de furnizorul sistemului de IA cu grad ridicat de risc în care sunt integrate sistemele, instrumentele, serviciile, componentele sau procesele lor de IA și ar trebui să îi ofere acestui furnizor, printr-un acord scris, informațiile, capacitățile, accesul tehnic și alte tipuri de asistență necesare bazate pe stadiul de avansare al tehnologiei general recunoscut, pentru a permite furnizorului să respecte pe deplin obligațiile prevăzute în prezentul regulament, fără a-și compromite propriile drepturi de proprietate intelectuală sau secrete comerciale.
- (89) Părțile terțe care pun la dispoziția publicului instrumente, servicii, procese sau componente de IA, altele decât modelele de IA de uz general, ar trebui să nu fie obligate să respecte cerințe care vizează responsabilitățile de-a lungul lanțului valoric al IA, în special față de furnizorul care le-a utilizat sau le-a integrat, atunci când aceste instrumente, servicii, procese sau componente de IA sunt puse la dispoziție sub licență liberă și deschisă. Dezvoltatorii de instrumente, servicii, procese sau componente de IA libere și cu sursă deschisă, altele decât modelele de IA de uz general, ar trebui să fie încurajați să pună în aplicare practici de documentare adoptate pe scară largă, cum ar fi carduri însoțitoare ale modelelor și fișe de date, ca modalitate de a accelera schimbul de informații de-a lungul lanțului valoric al IA, permițând promovarea unor sisteme de IA fiabile în Uniune.

- (90) Comisia ar putea elabora și recomanda un model voluntar de clauze contractuale între furnizorii de sisteme de IA cu grad ridicat de risc și părțile terțe care furnizează instrumente, servicii, componente sau procese care sunt utilizate sau integrate în sistemele de IA cu grad ridicat de risc, pentru a facilita cooperarea de-a lungul lanțului valoric. Atunci când elaborează modelul voluntar de clauze contractuale, Comisia ar trebui să ia în considerare și eventualele cerințe contractuale aplicabile în anumite sectoare sau situații economice.
- (91) Având în vedere natura sistemelor de IA și riscurile la adresa siguranței și a drepturilor fundamentale care pot fi asociate cu utilizarea lor, inclusiv în ceea ce privește necesitatea de a asigura o monitorizare adecvată a performanței unui sistem de IA într-un context real, este oportun să se stabilească responsabilități specifice pentru implementatori. Implementatorii ar trebui, în special, să ia măsurile tehnice și organizatorice adecvate pentru a se asigura că utilizează sisteme de IA cu grad ridicat de risc în conformitate cu instrucțiunile de utilizare și ar trebui să fie prevăzute și alte obligații în ceea ce privește monitorizarea funcționării sistemelor de IA și păstrarea evidențelor, după caz. În plus, implementatorii ar trebui să se asigure că persoanele desemnate să pună în aplicare instrucțiunile de utilizare și supravegherea umană, astfel cum sunt prevăzute în prezentul regulament, au competența necesară, în special un nivel adecvat de alfabetizare, formare și autoritate în domeniul IA pentru a îndeplini în mod corespunzător sarcinile respective. Respectivăle obligații nu ar trebui să aducă atingere altor obligații ale implementatorilor în ceea ce privește sistemele de IA cu grad ridicat de risc în temeiul dreptului Uniunii sau al dreptului intern.

(92) Prezentul regulament nu aduce atingere obligațiilor angajatorilor de a informa sau de a informa și consulta lucrătorii sau reprezentanții acestora în temeiul dreptului și al practicilor Uniunii sau naționale, inclusiv al Directivei 2002/14/CE a Parlamentului European și a Consiliului³⁹, cu privire la deciziile de punere în funcțiune sau de utilizare a sistemelor de IA. Este în continuare necesar să se asigure informarea lucrătorilor și a reprezentanților acestora cu privire la implementarea planificată a sistemelor de IA cu grad ridicat de risc la locul de muncă în cazul în care nu sunt îndeplinite condițiile pentru respectivele obligații de informare sau de informare și consultare prevăzute în alte instrumente juridice. În plus, un astfel de drept la informare este auxiliar și necesar în raport cu obiectivul de protecție a drepturilor fundamentale care stă la baza prezentului regulament. Prin urmare, prezentul regulament ar trebui să prevadă o cerință de informare în acest sens, fără a afecta drepturile existente ale lucrătorilor.

³⁹ Directiva 2002/14/CE a Parlamentului European și a Consiliului din 11 martie 2002 de stabilire a unui cadru general de informare și consultare a lucrătorilor din Comunitatea Europeană (JO L 80, 23.3.2002, p. 29).

(93) Deși riscurile legate de sistemele de IA pot rezulta din modul în care sunt proiectate sistemele respective, pot decurge riscuri și din modul în care aceste sisteme de IA sunt utilizate. Prin urmare, implementatorii sistemelor de IA cu grad ridicat de risc joacă un rol esențial în garantarea faptului că drepturile fundamentale sunt protejate, completând obligațiile furnizorului la dezvoltarea sistemului de IA. Implementatorii sunt cei mai în măsură să înțeleagă modul în care sistemul de IA cu grad ridicat de risc va fi utilizat concret și, prin urmare, pot identifica potențialele riscuri semnificative care nu au fost prevăzute în faza de dezvoltare, datorită cunoașterii mai exacte a contextului de utilizare, a persoanelor sau a grupurilor de persoane care ar putea fi afectate, inclusiv a grupurilor vulnerabile. Implementatorii de sisteme de IA cu grad ridicat de risc enumerate într-o anexă la prezentul regulament joacă, de asemenea, un rol esențial în informarea persoanelor fizice și ar trebui, atunci când iau decizii sau contribuie la luarea deciziilor referitoare la persoane fizice, după caz, să informeze persoanele fizice că fac obiectul utilizării sistemului de IA cu grad ridicat de risc. Aceste informații ar trebui să includă scopul urmărit și tipul de decizii luate. Implementatorul ar trebui, de asemenea, să informeze persoanele fizice cu privire la dreptul lor la o explicație furnizată în temeiul prezentului regulament. În ceea ce privește sistemele de IA cu grad ridicat de risc utilizate în scopul aplicării legii, această obligație ar trebui să fie pusă în aplicare în conformitate cu articolul 13 din Directiva (UE) 2016/680.

- (94) Orice prelucrare a datelor biometrice implicate în utilizarea sistemelor de IA pentru identificarea biometrică în scopul aplicării legii trebuie să respecte articolul 10 din Directiva (UE) 2016/680, care permite o astfel de prelucrare numai atunci când este strict necesară, sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate, și atunci când este autorizată de dreptul Uniunii sau de dreptul intern. O astfel de utilizare, atunci când este autorizată, trebuie, de asemenea, să respecte principiile prevăzute la articolul 4 alineatul (1) din Directiva (UE) 2016/680, inclusiv legalitatea, echitatea și transparența, limitarea scopului, exactitatea și limitarea stocării.
- (95) Fără a aduce atingere dreptului aplicabil al Uniunii, în special Regulamentului (UE) 2016/679 și Directivei (UE) 2016/680, având în vedere caracterul intruziv al sistemelor de identificare biometrică la distanță ulterioară, utilizarea sistemelor de identificare biometrică la distanță ulterioară ar trebui să facă obiectul unor garanții. Sistemele de identificare biometrică la distanță ulterioară ar trebui să fie utilizate întotdeauna într-un mod proporțional, legitim și strict necesar și, prin urmare, adaptat, în ceea ce privește persoanele care urmează să fie identificate, localizarea, acoperirea temporală și pe baza unui set de date închis de înregistrări video obținute în mod legal. În orice caz, sistemele de identificare biometrică la distanță ulterioară nu ar trebui să fie utilizate în cadrul aplicării legii pentru a conduce la o supraveghere arbitrară. Condițiile pentru identificarea biometrică la distanță ulterioară nu ar trebui, în niciun caz, să ofere o bază pentru a eluda condițiile interdicției și excepțiile stricte pentru identificarea biometrică la distanță în timp real.

- (96) Pentru a se asigura în mod eficient că drepturile fundamentale sunt protejate, implementatorii de sisteme de IA cu grad ridicat de risc care sunt organisme de drept public sau entitățile private care furnizează servicii publice și implementatorii care implementează anumite sisteme de IA cu grad ridicat de risc enumerate într-o anexă la prezentul regulament, cum ar fi entitățile bancare sau de asigurări, ar trebui să efectueze o evaluare a impactului asupra drepturilor fundamentale înainte de a pune aceste sisteme în funcțiune. Serviciile importante pentru persoanele fizice care sunt de natură publică pot fi furnizate și de entități private. Entitățile private care furnizează astfel de servicii publice sunt legați de sarcini de interes public, cum ar fi în domeniul educației, al îngrijirilor de sănătate, al serviciilor sociale, al locuințelor, al administrării justiției. Scopul evaluării impactului asupra drepturilor fundamentale este ca implementatorul să identifice riscurile specifice pentru drepturile persoanelor sau ale grupurilor de persoane care ar putea fi afectate și să identifice măsurile care trebuie luate în cazul materializării riscurilor respective. Evaluarea impactului ar trebui să fie efectuată înainte de implementarea sistemului de IA cu grad ridicat de risc și ar trebui să fie actualizată atunci când implementatorul consideră că oricare dintre factorii relevanți s-au schimbat. Evaluarea impactului ar trebui să identifice procesele relevante ale implementatorului în care sistemul de IA cu grad ridicat de risc va fi utilizat în conformitate cu scopul său preconizat și ar trebui să includă o descriere a perioadei de timp și a frecvenței în care se intenționează utilizarea sistemului, precum și a categoriilor specifice de persoane fizice și grupuri care sunt susceptibile de a fi afectate în contextul specific de utilizare.

Evaluarea ar trebui să includă, de asemenea, identificarea riscurilor specifice de prejudiciu care ar putea avea un impact asupra drepturilor fundamentale ale persoanelor sau grupurilor respective. Atunci când efectuează această evaluare, implementatorul ar trebui să țină seama de informațiile relevante pentru o evaluare adecvată a impactului, inclusiv de informațiile furnizate de furnizorul sistemului de IA cu grad ridicat de risc în instrucțiunile de utilizare, dar fără a se limita la aceste informații. Având în vedere riscurile identificate, implementatorii ar trebui să stabilească măsurile care trebuie luate în cazul materializării acestor riscuri, inclusiv, de exemplu, mecanisme de guvernare în acest context specific de utilizare, cum ar fi mecanisme de supraveghere umană în conformitate cu instrucțiunile de utilizare sau proceduri de tratare a plângerilor și proceduri aferente măsurilor reparatorii, deoarece acestea ar putea fi esențiale pentru atenuarea riscurilor la adresa drepturilor fundamentale în cazuri concrete de utilizare. După efectuarea respectivei evaluări a impactului, implementatorul ar trebui să îi notifice acest lucru autorității relevante de supraveghere a pieței. După caz, pentru a colecta informațiile relevante necesare pentru efectuarea evaluării impactului, implementatorii de sisteme de IA cu grad ridicat de risc, în special atunci când sistemele de IA sunt utilizate în sectorul public, ar putea implica părțile interesate relevante, inclusiv reprezentanții grupurilor de persoane susceptibile de a fi afectate de sistemul de IA, experții independenți și organizațiile societății civile în efectuarea unor astfel de evaluări ale impactului și în conceperea măsurilor care trebuie luate în cazul materializării riscurilor. Oficiul european pentru inteligența artificială (Oficiul pentru IA) ar trebui să elaboreze un model de chestionar pentru a facilita conformitatea și a reduce sarcina administrativă pentru implementatori.

- (97) Noțiunea de modele de IA de uz general ar trebui să fie definită în mod clar și separată de noțiunea de sisteme de IA pentru a asigura securitatea juridică. Definiția ar trebui să se bazeze pe caracteristicile funcționale esențiale ale unui model de IA de uz general, în special pe generalitate și pe capacitatea de a îndeplini în mod competent o gamă largă de sarcini distincte. Aceste modele sunt, de regulă, antrenate pe volume mari de date, prin diverse metode, cum ar fi învățarea autosupravegheată, nesupravegheată sau prin întărire. Modelele de IA de uz general pot fi introduse pe piață în diferite moduri, inclusiv prin biblioteci, interfețe de programare a aplicațiilor (API), sub formă de descărcare directă sau sub formă de copie fizică. Aceste modele pot fi modificate suplimentar sau calibrate și astfel transformate în modele noi. Deși modelele de IA sunt componente esențiale ale sistemelor de IA, ele nu constituie sisteme de IA în sine. Modelele de IA necesită adăugarea de componente suplimentare, cum ar fi, de exemplu, o interfață cu utilizatorul, pentru a deveni sisteme de IA. Modelele de IA sunt, de regulă, integrate în sistemele de IA și fac parte din acestea. Prezentul regulament prevede norme specifice pentru modelele de IA de uz general și pentru modelele de IA de uz general care prezintă riscuri sistemice, norme care ar trebui să se aplice și atunci când aceste modele sunt integrate sau fac parte dintr-un sistem de IA. Ar trebui să se înțeleagă că obligațiile furnizorilor de modele de IA de uz general ar trebui să se aplice odată ce modelele de IA de uz general sunt introduse pe piață.

Atunci când furnizorul unui model de IA de uz general integrează un model propriu în propriul sistem de IA care este pus la dispoziție pe piață sau pus în funcțiune, modelul respectiv ar trebui să fie considerat ca fiind introdus pe piață și, prin urmare, obligațiile prevăzute în prezentul regulament pentru modele ar trebui să se aplice în continuare în plus față de cele pentru sistemele de IA. Obligațiile stabilite pentru modele nu ar trebui în niciun caz să se aplice atunci când un model propriu este utilizat pentru procese pur interne care nu sunt esențiale pentru furnizarea unui produs sau a unui serviciu către terți, iar drepturile persoanelor fizice nu sunt afectate. Având în vedere potențialele lor efecte negative semnificative, modelele de IA de uz general cu risc sistemic ar trebui să facă întotdeauna obiectul obligațiilor relevante în temeiul prezentului regulament. Definiția nu ar trebui să acopere modelele de IA utilizate înainte de introducerea lor pe piață în scopul unic al activităților de cercetare, dezvoltare și creare de prototipuri. Acest lucru nu aduce atingere obligației de a se conforma prezentului regulament atunci când, în urma unor astfel de activități, se introduce pe piață un model.

- (98) În timp ce generalitatea unui model ar putea fi determinată, printre altele, și de o serie de parametri, ar trebui să se considere că modelele cu cel puțin un miliard de parametri și antrenate cu un volum mare de date utilizând autosupravegherea la scară largă prezintă o generalitate semnificativă și îndeplinesc în mod competent o gamă largă de sarcini distincte.
- (99) Modelele de IA generative de mari dimensiuni sunt un exemplu tipic de model de IA de uz general, având în vedere că permit generarea flexibilă de conținut, cum ar fi sub formă de text, audio, imagini sau video, care pot răspunde cu ușurință unei game largi de sarcini distincte.

- (100) Atunci când un model de IA de uz general este integrat într-un sistem de IA sau face parte dintr-un astfel de sistem, acest sistem ar trebui să fie considerat a fi un sistem de IA de uz general atunci când, în urma acestei integrări, acest sistem are capacitatea de a servi unei varietăți de scopuri. Un sistem de IA de uz general poate fi utilizat direct sau poate fi integrat în alte sisteme de IA.
- (101) Furnizorii de modele de IA de uz general au un rol și o responsabilitate deosebite de-a lungul lanțului valoric al IA, deoarece modelele pe care le furnizează pot constitui baza pentru o serie de sisteme din aval, adesea furnizate de furnizori din aval care au nevoie de o bună înțelegere a modelelor și a capacităților acestora, atât pentru a permite integrarea unor astfel de modele în produsele lor, cât și pentru a-și îndeplini obligațiile care le revin în temeiul prezentului regulament sau al altor regulamente. Prin urmare, ar trebui să fie stabilite măsuri proporționale de transparență, inclusiv întocmirea și ținerea la zi a documentației, precum și furnizarea de informații privind modelul de IA de uz general pentru utilizarea sa de către furnizorii din aval. Documentația tehnică ar trebui să fie pregătită și ținută la zi de către furnizorul modelului de IA de uz general în scopul de a o pune, la cerere, la dispoziția Oficiului pentru IA și a autorităților naționale competente. Setul minim de elemente care trebuie incluse în această documentație ar trebui să fie stabilit în anexele specifice la prezentul regulament. Comisia ar trebui să fie împuternicită să modifice anexele respective prin intermediul unor acte delegate în funcție de evoluțiile tehnologice.

- (102) Software-ul și datele, inclusiv modelele, lansate sub licență liberă și cu sursă deschisă care le permite să fie partajate în mod deschis și pe care utilizatorii le pot accesa, utiliza, modifica și redistribui liber sau versiuni modificate ale acestora, pot contribui la cercetare și inovare pe piață și pot oferi oportunități semnificative de creștere pentru economia Uniunii. Ar trebui să se considere că modelele de IA de uz general lansate sub licențe libere și cu sursă deschisă asigură niveluri ridicate de transparență și deschidere dacă parametrii lor, inclusiv ponderile, informațiile privind arhitectura modelului și informațiile privind utilizarea modelului, sunt puși la dispoziția publicului. Licența ar trebui să fie considerată ca fiind liberă și cu sursă deschisă și atunci când le permite utilizatorilor să ruleze, să copieze, să distribuie, să studieze, să modifice și să îmbunătățească software-ul și datele, inclusiv modelele, cu condiția ca furnizorul inițial al modelului să fie menționat și ca termenii de distribuție identici sau comparabili să fie respectați.
- (103) Componentele de IA libere și cu sursă deschisă acoperă software-ul și datele, inclusiv modelele și modelele, instrumentele, serviciile sau procesele de IA de uz general ale unui sistem de IA. Componentele de IA libere și cu sursă deschisă pot fi furnizate prin diferite canale, inclusiv prin dezvoltarea lor în depozite deschise. În sensul prezentului regulament, componentele de IA care sunt furnizate contra unui preț sau monetizate în alt mod, inclusiv prin furnizarea de sprijin tehnic sau de alte servicii, inclusiv prin intermediul unei platforme software, legate de componenta de IA, sau utilizarea datelor cu caracter personal din alte motive decât în scopul exclusiv de îmbunătățire a securității, a compatibilității sau a interoperabilității software-ului, cu excepția tranzacțiilor dintre microîntreprinderi, nu ar trebui să beneficieze de excepțiile prevăzute pentru componentele de IA libere și cu sursă deschisă. Punerea la dispoziție a componentelor de IA prin intermediul depozitelor deschise nu ar trebui, în sine, să constituie o monetizare.

- (104) Furnizorii de modele de IA de uz general care sunt lansate sub licență liberă și cu sursă deschisă și ai căror parametri, inclusiv ponderile, informațiile privind arhitectura modelului și informațiile privind utilizarea modelului, sunt puși la dispoziția publicului ar trebui să facă obiectul unor excepții în ceea ce privește cerințele legate de transparență impuse modelelor de IA de uz general, cu excepția cazului în care se poate considera că prezintă un risc sistemic, caz în care circumstanța că modelul este transparent și însoțit de o licență cu sursă deschisă nu ar trebui să fie considerată un motiv suficient pentru a exclude respectarea obligațiilor prevăzute în prezentul regulament. În orice caz, având în vedere că lansarea modelelor de IA de uz general sub licență liberă și cu sursă deschisă nu dezvăluie neapărat informații substanțiale cu privire la setul de date utilizat pentru antrenarea sau calibrarea modelului și la modul în care a fost astfel asigurată conformitatea cu dreptul privind drepturile de autor, excepția prevăzută pentru modelele de IA de uz general de la respectarea cerințelor legate de transparență nu ar trebui să se refere la obligația de a prezenta un rezumat cu privire la conținutul utilizat pentru antrenarea modelelor și la obligația de a institui o politică de respectare a dreptului Uniunii privind drepturile de autor, în special pentru a identifica și a respecta rezervarea drepturilor în temeiul articolului 4 alineatul (3) din Directiva (UE) 2019/790 a Parlamentului European și a Consiliului⁴⁰.

⁴⁰ Directiva (UE) 2019/790 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind dreptul de autor și drepturile conexe pe piața unică digitală și de modificare a Directivelor 96/9/CE și 2001/29/CE (JO L 130, 17.5.2019, p. 92).

- (105) Modelele de IA de uz general, în special modelele de IA generative de mari dimensiuni, capabile să genereze text, imagini și alte conținuturi, prezintă oportunități unice de inovare, dar și provocări pentru artiști, autori și alți creatori și pentru modul în care conținutul lor creativ este creat, distribuit, utilizat și consumat. Dezvoltarea și antrenarea unor astfel de modele necesită acces la volume mari de text, imagini, materiale video și alte date. Tehnicile de extragere a textului și a datelor pot fi utilizate pe scară largă în acest context pentru obținerea și analizarea unui astfel de conținut, care poate fi protejat prin drepturi de autor și drepturi conexe. Orice utilizare a unui conținut protejat prin drepturi de autor necesită autorizare din partea titularului de drepturi în cauză, cu excepția cazului în care se aplică excepții și limitări relevante ale drepturilor de autor. Directiva (UE) 2019/790 a introdus excepții și limitări care permit reproducere și extrageri ale operelor sau ale altor obiecte protejate, în scopul extragerii de text și de date, în anumite condiții. În temeiul acestor norme, titularii de drepturi pot alege să își rezerve drepturile asupra operelor lor sau asupra altor obiecte protejate ale lor pentru a preveni extragerea de text și de date, cu excepția cazului în care acest lucru se face în scopul cercetării științifice. În cazul în care drepturile de neparticipare au fost rezervate în mod expres într-un mod adecvat, furnizorii de modele de IA de uz general trebuie să obțină o autorizație din partea titularilor de drepturi dacă doresc să efectueze extragere de text și de date din astfel de opere.

- (106) Furnizorii care introduc modele de IA de uz general pe piața Uniunii ar trebui să asigure respectarea obligațiilor relevante prevăzute în prezentul regulament. În acest scop, furnizorii de modele de IA de uz general ar trebui să instituie o politică de respectare a dreptului Uniunii privind drepturile de autor și drepturile conexe, în special pentru a identifica și a respecta rezervarea drepturilor exprimată de titularii de drepturi în temeiul articolului 4 alineatul (3) din Directiva (UE) 2019/790. Orice furnizor care introduce un model de IA de uz general pe piața Uniunii ar trebui să respecte această obligație, indiferent de jurisdicția în care au loc actele relevante pentru drepturile de autor care stau la baza antrenării respectivelor modele de IA de uz general. Acest lucru este necesar pentru a asigura condiții de concurență echitabile între furnizorii de modele de IA de uz general, în care niciun furnizor nu ar trebui să poată obține un avantaj competitiv pe piața Uniunii prin aplicarea unor standarde privind drepturile de autor mai scăzute decât cele prevăzute în Uniune.

- (107) Pentru a spori transparența datelor utilizate în preantrenarea și antrenarea modelelor de IA de uz general, inclusiv a textului și a datelor protejate de dreptul privind drepturile de autor, este adecvat ca furnizorii de astfel de modele să elaboreze și să pună la dispoziția publicului un rezumat suficient de detaliat al conținutului utilizat pentru antrenarea modelului de IA de uz general. Ținând seama în mod corespunzător de necesitatea de a proteja secretele comerciale și informațiile comerciale confidențiale, acest rezumat ar trebui să aibă un domeniu de aplicare în general cuprinzător, în loc să fie detaliat din punct de vedere tehnic, pentru a facilita părților cu interese legitime, inclusiv titularilor de drepturi de autor, să își exercite drepturile și să asigure respectarea drepturilor lor în temeiul dreptului Uniunii, de exemplu prin enumerarea principalelor colecții sau seturi de date folosite la antrenarea modelului, cum ar fi bazele de date sau arhivele de date de mari dimensiuni, private sau publice, și prin furnizarea unei explicații narative cu privire la alte surse de date utilizate. Este oportun ca Oficiul pentru IA să furnizeze un model pentru rezumat, care ar trebui să fie simplu, eficient și să permită furnizorului să furnizeze rezumatul solicitat sub formă narativă.
- (108) În ceea ce privește obligațiile impuse furnizorilor de modele de IA de uz general de a institui o politică de respectare a dreptului Uniunii privind drepturile de autor și de a pune la dispoziția publicului un rezumat al conținutului utilizat pentru antrenare, Oficiul pentru IA ar trebui să monitorizeze dacă furnizorul și-a îndeplinit obligațiile respective fără a verifica sau a efectua o evaluare operă cu operă a datelor de antrenament în ceea ce privește respectarea drepturilor de autor. Prezentul regulament nu aduce atingere aplicării normelor în materie de drepturi de autor prevăzute în dreptul Uniunii.

- (109) Respectarea obligațiilor aplicabile furnizorilor de modele de IA de uz general ar trebui să fie corespunzătoare și proporțională cu tipul de furnizor de model, excluzând necesitatea respectării pentru persoanele care dezvoltă sau utilizează modele în alte scopuri decât cele profesionale sau de cercetare științifică, care ar trebui totuși să fie încurajate să respecte în mod voluntar aceste cerințe. Fără a aduce atingere dreptului Uniunii privind drepturile de autor, respectarea obligațiilor respective ar trebui să țină seama în mod corespunzător de dimensiunea furnizorului și să permită modalități simplificate de asigurare a respectării cerințelor pentru IMM-uri, inclusiv pentru întreprinderile nou-înființate, care nu ar trebui să reprezinte un cost excesiv și să descurajeze utilizarea unor astfel de modele. În cazul unei modificări sau calibrări a unui model, obligațiile furnizorilor de modele de IA de uz general ar trebui să se limiteze la modificarea sau calibrarea respectivă, de exemplu prin completarea documentației tehnice deja existente cu informații privind modificările, inclusiv noi surse de date de antrenament, ca mijloc de respectare a obligațiilor privind lanțul valoric prevăzute în prezentul regulament.

- (110) Modelele de IA de uz general ar putea prezenta riscuri sistemice care includ, printre altele, orice efecte negative reale sau previzibile în mod rezonabil în legătură cu accidente majore, perturbări ale sectoarelor critice și consecințe grave pentru sănătatea și siguranța publică, orice efecte negative reale sau previzibile în mod rezonabil asupra proceselor democratice, asupra securității publice și economice, diseminarea de conținut ilegal, fals sau discriminatoriu. Riscurile sistemice ar trebui să fie înțelese ca crescând odată cu capabilitățile modelului și cu amploarea modelului, pot apărea de-a lungul întregului ciclu de viață al modelului și sunt influențate de condițiile de utilizare necorespunzătoare, de fiabilitatea modelului, de echitatea modelului și de securitatea modelului, de nivelul de autonomie a modelului, de accesul său la instrumente, de modalitățile noi sau combinate, de strategiile de lansare și distribuție, de potențialul de eliminare a mecanismelor de protecție și de alți factori. În special, abordările internaționale au identificat până în prezent necesitatea de a acorda atenție riscurilor generate de potențialele utilizări necorespunzătoare intenționate sau de problemele neintenționate de control legate de alinierea la intenția umană; riscurilor chimice, biologice, radiologice și nucleare, cum ar fi modalitățile de reducere a barierelor la intrare, inclusiv pentru dezvoltarea, proiectarea, achiziționarea sau utilizarea de arme; capabilităților cibernetice ofensive, cum ar fi modalitățile care permit descoperirea, exploatarea sau utilizarea operațională a vulnerabilităților; efectelor interacțiunii și ale utilizării instrumentelor, inclusiv, de exemplu, capacitatea de a controla sistemele fizice și de a interfera cu infrastructura critică; riscurilor legate de posibilitatea ca modelele să facă copii după ele însele sau să se „autoreproducă” ori să antreneze alte modele; modurilor în care modelele pot da naștere unor prejudecăți dăunătoare și discriminării cu riscuri pentru indivizi, comunități sau societăți; facilitării dezinformării sau prejudicierii vieții private cu amenințări la adresa valorilor democratice și a drepturilor omului; riscului ca un anumit eveniment să conducă la o reacție în lanț cu efecte negative considerabile care ar putea afecta până la un întreg oraș, o întreagă activitate de domeniu sau o întreagă comunitate.

- (111) Este oportun să se stabilească o metodologie pentru clasificarea modelelor de IA de uz general ca modele de IA de uz general cu riscuri sistemice. Întrucât riscurile sistemice rezultă din capabilități deosebit de ridicate, ar trebui să se considere că un model de IA de uz general prezintă riscuri sistemice dacă are capabilități cu impact ridicat, evaluate pe baza unor instrumente și metodologii tehnice adecvate sau dacă are un impact semnificativ asupra pieței interne din cauza amplitudinii sale. Capabilități cu impact ridicat în modelele de IA de uz general înseamnă capabilități care corespund capabilităților înregistrate în cele mai avansate modele de IA de uz general sau depășesc capabilitățile respective. Întreaga gamă de capabilități ale unui model ar putea fi mai bine înțeleasă după introducerea sa pe piață sau atunci când implementatorii interacționează cu modelul. În conformitate cu stadiul actual al tehnologiei la momentul intrării în vigoare a prezentului regulament, volumul cumulat de calcul utilizat pentru antrenarea modelului de IA de uz general măsurat în operații în virgulă mobilă este una dintre aproximările relevante pentru capabilitățile modelului. Volumul cumulat de calcul utilizat pentru antrenare include calculul utilizat pentru toate activitățile și metodele menite să consolideze capabilitățile modelului înainte de implementare, cum ar fi preantrenarea, generarea de date sintetice și calibrarea. Prin urmare, ar trebui să fie stabilit un prag inițial de operații în virgulă mobilă, care, dacă este atins de un model de IA de uz general, conduce la prezumția că modelul este un model de IA de uz general cu riscuri sistemice. Acest prag ar trebui să fie ajustat în timp pentru a reflecta schimbările tehnologice și industriale, cum ar fi îmbunătățirile algoritmice sau eficiența hardware sporită, și ar trebui să fie completat cu valori de referință și indicatori pentru capabilitatea modelului.

În acest scop, Oficiul pentru IA ar trebui să colaboreze cu comunitatea științifică, cu industria, cu societatea civilă și cu alți experți. Pragurile, precum și instrumentele și valorile de referință pentru evaluarea capabilităților cu impact ridicat ar trebui să fie indicatori puternici ai generalității, ai capabilităților modelului și ai riscului sistemic asociat modelelor de IA de uz general și ar putea lua în considerare modul în care modelul va fi introdus pe piață sau numărul de utilizatori pe care îi poate afecta. Pentru a completa acest sistem, Comisia ar trebui să aibă posibilitatea de a lua decizii individuale de desemnare a unui model de IA de uz general ca model de IA de uz general cu risc sistemic dacă se constată că un astfel de model are capabilități sau un impact echivalent cu cele acoperite de pragul stabilit. Decizia respectivă ar trebui luată pe baza unei evaluări globale a criteriilor pentru desemnarea unui model de IA de uz general cu risc sistemic prevăzute într-o anexă la prezentul regulament, cum ar fi calitatea sau dimensiunea setului de date de antrenament, numărul de utilizatori comerciali și finali, modalitățile referitoare la datele de intrare și de ieșire ale modelului, nivelul său de autonomie și de scalabilitate sau instrumentele la care are acces. La cererea motivată a unui furnizor al cărui model a fost desemnat drept model de IA de uz general cu risc sistemic, Comisia ar trebui să țină seama de cerere și poate decide să reevalueze dacă modelul de IA de uz general poate fi considerat în continuare ca prezentând riscuri sistemice.

- (112) De asemenea, este necesar să se clarifice o procedură pentru clasificarea unui model de IA de uz general cu riscuri sistemice. Un model de IA de uz general care respectă pragul aplicabil pentru capabilitățile cu impact ridicat ar trebui să fie prezumat ca fiind un model de IA de uz general cu risc sistemic. Furnizorul ar trebui să notifice Oficiul pentru IA în termen de cel mult două săptămâni de la îndeplinirea cerințelor sau de la data la care devine cunoscut faptul că un model de IA de uz general va îndeplini cerințele care conduc la prezumția respectivă. Acest lucru este deosebit de relevant în legătură cu pragul de operații în virgulă mobilă, deoarece antrenarea modelelor de IA de uz general necesită o planificare considerabilă, care include alocarea în avans a resurselor de calcul și, prin urmare, furnizorii de modele de IA de uz general sunt în măsură să știe dacă modelul lor ar atinge pragul înainte de finalizarea antrenării. În contextul notificării respective, furnizorul ar trebui să poată demonstra că, având în vedere caracteristicile sale specifice, un model de IA de uz general nu prezintă, în mod excepțional, riscuri sistemice și că, prin urmare, nu ar trebui să fie clasificat drept model de IA de uz general cu riscuri sistemice. Aceste informații sunt valoroase deoarece Oficiul pentru IA poate să anticipeze introducerea pe piață a modelelor de IA de uz general cu riscuri sistemice, iar furnizorii pot începe să colaboreze cu Oficiul pentru IA din timp. Aceste informații sunt deosebit de importante în ceea ce privește modelele de IA de uz general care sunt planificate să fie lansate ca sursă deschisă, având în vedere că, după lansarea modelului cu sursă deschisă, măsurile necesare pentru a asigura respectarea obligațiilor prevăzute în prezentul regulament pot fi mai dificil de pus în aplicare.

- (113) În cazul în care Comisia constată că un model de IA de uz general îndeplinește cerințele de clasificare ca model de IA de uz general cu risc sistemic, lucru care anterior fie nu fusese cunoscut, fie nu fusese notificat Comisiei de furnizorul relevant, Comisia ar trebui să fie împuternicită să îl desemneze ca atare. Un sistem de alerte calificate ar trebui să asigure faptul că Oficiul pentru IA este informat de către grupul științific cu privire la modele de IA de uz general care ar putea fi clasificate drept modele de IA de uz general cu risc sistemic, pe lângă activitățile de monitorizare ale Oficiului pentru IA.
- (114) Furnizorii de modele de IA de uz general care prezintă riscuri sistemice ar trebui să facă obiectul, pe lângă obligațiile prevăzute pentru furnizorii de modele de IA de uz general, unor obligații menite să identifice și să atenueze riscurile respective și să asigure un nivel adecvat de protecție în materie de securitate cibernetică, indiferent dacă este furnizat ca model de sine stătător sau încorporat într-un sistem sau într-un produs de IA. Pentru a atinge obiectivele respective, prezentul regulament ar trebui să impună furnizorilor să efectueze evaluările necesare ale modelelor, în special înainte de prima lor introducere pe piață, inclusiv efectuarea și documentarea testării contradictorii a modelelor, inclusiv, după caz, prin testări interne sau externe independente. În plus, furnizorii de modele de IA de uz general cu riscuri sistemice ar trebui să evalueze și să atenueze în permanență riscurile sistemice, inclusiv, de exemplu, prin instituirea unor politici de gestionare a riscurilor, cum ar fi procesele de asigurare a răspunderii și de guvernanță, prin punerea în aplicare a monitorizării ulterioare introducerii pe piață, prin luarea de măsuri adecvate de-a lungul întregului ciclu de viață al modelului și prin cooperarea cu actorii relevanți de-a lungul lanțului valoric al IA.

- (115) Furnizorii de modele de IA de uz general cu riscuri sistemice ar trebui să evalueze și să atenueze posibilele riscuri sistemice. Dacă, în pofida eforturilor de identificare și prevenire a riscurilor legate de un model de IA de uz general care poate prezenta riscuri sistemice, dezvoltarea sau utilizarea modelului cauzează un incident grav, furnizorul modelului de IA de uz general ar trebui să urmărească fără întârzieri nejustificate incidentul și să raporteze Comisiei și autorităților naționale competente orice informații relevante și posibile măsuri corective. În plus, furnizorii ar trebui să asigure un nivel adecvat de protecție în materie de securitate cibernetică pentru model și infrastructura fizică a acestuia, dacă este cazul, de-a lungul întregului ciclu de viață al modelului. Protecția în materie de securitate cibernetică legată de riscurile sistemice asociate utilizării răuvoitoare sau atacurilor ar trebui să ia în considerare în mod corespunzător scurgerile accidentale de modele, lansările neautorizate, eludarea măsurilor de siguranță și apărarea împotriva atacurilor cibernetice, a accesului neautorizat sau a furtului de modele. Această protecție ar putea fi facilitată prin securizarea ponderilor modelelor, a algoritmilor, a serverelor și a seturilor de date, de exemplu prin măsuri de securitate operațională pentru securitatea informațiilor, politici specifice în materie de securitate cibernetică, soluții tehnice și consacrate adecvate și controale ale accesului cibernetic și fizic, adecvate circumstanțelor relevante și riscurilor implicate.

- (116) Oficiul pentru IA ar trebui să încurajeze și să faciliteze elaborarea, revizuirea și adaptarea unor coduri de bune practici, ținând seama de abordările internaționale. Toți furnizorii de modele de IA de uz general ar putea fi invitați să participe. Pentru a se asigura că codurile de bune practici reflectă stadiul actual al tehnologiei și țin seama în mod corespunzător de un set divers de perspective, Oficiul pentru IA ar trebui să colaboreze cu autoritățile naționale competente relevante și ar putea, după caz, să se consulte cu organizațiile societății civile și cu alte părți interesate și experți relevanți, inclusiv cu grupul științific, pentru elaborarea unor astfel de coduri. Codurile de bune practici ar trebui să se refere la obligațiile furnizorilor de modele de IA de uz general și de modele de IA de uz general care prezintă riscuri sistemice. În plus, în ceea ce privește riscurile sistemice, codurile de bune practici ar trebui să contribuie la stabilirea unei taxonomii a tipurilor și naturii riscurilor sistemice la nivelul Uniunii, inclusiv a surselor acestora. Codurile de bune practici ar trebui să se axeze, de asemenea, pe măsuri specifice de evaluare și de atenuare a riscurilor.

- (117) Codurile de bune practici ar trebui să reprezinte un instrument central pentru respectarea corespunzătoare a obligațiilor prevăzute în prezentul regulament pentru furnizorii de modele de IA de uz general. Furnizorii ar trebui să se poată baza pe coduri de bune practici pentru a demonstra respectarea obligațiilor. Prin intermediul unor acte de punere în aplicare, Comisia poate decide să aprobe un cod de bune practici și să îi acorde o valabilitate generală în Uniune sau, alternativ, să prevadă norme comune pentru punerea în aplicare a obligațiilor relevante, în cazul în care, până la momentul în care prezentul regulament devine aplicabil, un cod de bune practici nu poate fi finalizat sau nu este considerat adecvat de către Oficiul pentru IA. Odată ce un standard armonizat este publicat și evaluat ca fiind adecvat pentru a acoperi obligațiile relevante de către Oficiul pentru IA, furnizorii ar trebui să beneficieze de prezumția de conformitate în cazul în care respectă un standard european armonizat. În plus, furnizorii de modele de IA de uz general ar trebui să poată demonstra conformitatea utilizând mijloace alternative adecvate, dacă nu sunt disponibile coduri de bune practici sau standarde armonizate sau dacă aleg să nu se bazeze pe acestea.

(118) Prezentul regulament reglementează sistemele de IA și modelele de IA prin impunerea anumitor cerințe și obligații pentru actorii relevanți de pe piață care le introduc pe piață, le pun în funcțiune sau le utilizează în Uniune, completând astfel obligațiile pentru furnizorii de servicii intermediare care încorporează astfel de sisteme sau modele în serviciile lor reglementate de Regulamentul (UE) 2022/2065. În măsura în care astfel de sisteme sau modele sunt încorporate în platforme online foarte mari sau în motoare de căutare online foarte mari desemnate, acestea fac obiectul cadrului de gestionare a riscurilor prevăzut în Regulamentul (UE) 2022/2065. În consecință, ar trebui să se presupună că obligațiile corespunzătoare din prezentul regulament sunt îndeplinite, cu excepția cazului în care apar riscuri sistemice semnificative care nu intră sub incidența Regulamentului (UE) 2022/2065 și sunt identificate în astfel de modele. În acest cadru, furnizorii de platforme online foarte mari și de motoare de căutare online foarte mari sunt obligați să evalueze potențialele riscuri sistemice care decurg din proiectarea, funcționarea și utilizarea serviciilor lor, inclusiv modul în care proiectarea sistemelor algoritmice utilizate în cadrul serviciului poate contribui la astfel de riscuri, precum și riscurile sistemice care decurg din potențialele utilizări necorespunzătoare. Acești furnizori sunt, de asemenea, obligați să ia măsuri adecvate de atenuare, cu respectarea drepturilor fundamentale.

- (119) Având în vedere ritmul rapid al inovării și al evoluției tehnologice a serviciilor digitale care intră în domeniul de aplicare al diferitelor instrumente din dreptul Uniunii, în special având în vedere utilizarea și percepția destinatarilor lor, sistemele de IA care fac obiectul prezentului regulament pot fi furnizate ca servicii intermediare sau ca părți ale acestora în sensul Regulamentului (UE) 2022/2065, care ar trebui să fie interpretat într-un mod neutru din punct de vedere tehnologic. De exemplu, sistemele de IA pot fi utilizate pentru a furniza motoare de căutare online, în special în măsura în care un sistem de IA, cum ar fi un chatbot online, efectuează căutări, în principiu, pe toate site-urile web, apoi încorporează rezultatele în cunoștințele sale existente și utilizează cunoștințele actualizate pentru a genera un singur rezultat care combină diferite surse de informații.
- (120) În plus, obligațiile impuse prin prezentul regulament furnizorilor și implementatorilor anumitor sisteme de IA pentru a permite detectarea și divulgarea faptului că rezultatele sistemelor respective sunt generate sau manipulate artificial sunt deosebit de relevante pentru a facilita punerea în aplicare efectivă a Regulamentului (UE) 2022/2065. Acest lucru este valabil în special în ceea ce privește obligațiile furnizorilor de platforme online foarte mari sau de motoare de căutare online foarte mari de a identifica și a atenua riscurile sistemice care pot apărea în urma diseminării conținutului care a fost generat sau manipulat artificial, în special riscul privind efectele negative reale sau previzibile asupra proceselor democratice, asupra discursului civic și asupra proceselor electorale, inclusiv prin dezinformare.

(121) Standardizarea ar trebui să joace un rol esențial în furnizarea de soluții tehnice furnizorilor pentru a asigura conformitatea cu prezentul regulament, în conformitate cu stadiul actual al tehnologiei, pentru a promova inovarea, precum și competitivitatea și creșterea pe piața unică. Conformitatea cu standardele armonizate, astfel cum sunt definite la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului⁴¹, care ar trebui, în mod normal, să reflecte stadiul actual al tehnologiei, ar trebui să fie un mijloc prin care furnizorii să demonstreze conformitatea cu cerințele prezentului regulament. Prin urmare, ar trebui să fie încurajată o reprezentare echilibrată a intereselor, care să implice toate părțile interesate relevante în elaborarea standardelor, în special IMM-urile, organizațiile consumatorilor și părțile interesate din domeniul mediului și din domeniul social, în conformitate cu articolele 5 și 6 din Regulamentul (UE) nr. 1025/2012. Pentru a facilita conformitatea, solicitările de standardizare ar trebui să fie emise de Comisie fără întârzieri nejustificate. Atunci când elaborează solicitarea de standardizare, Comisia ar trebui să consulte forumul consultativ și Consiliul IA pentru a colecta cunoștințele de specialitate relevante. Cu toate acestea, în absența unor trimiteri relevante la standardele armonizate, Comisia ar trebui să poată stabili, prin intermediul unor acte de punere în aplicare și după consultarea forumului consultativ, specificații comune pentru anumite cerințe în temeiul prezentului regulament.

⁴¹ Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului (JO L 316, 14.11.2012, p. 12).

Specificația comună ar trebui să constituie o soluție excepțională de rezervă, pentru a facilita obligația furnizorului de a respecta cerințele prezentului regulament, atunci când solicitarea de standardizare nu a fost acceptată de niciuna dintre organizațiile de standardizare europene sau când standardele armonizate relevante abordează insuficient preocupările în materie de drepturi fundamentale ori când standardele armonizate nu corespund solicitării sau atunci când există întârzieri în adoptarea unui standard armonizat adecvat. În cazul în care o astfel de întârziere în adoptarea unui standard armonizat se datorează complexității tehnice a standardului respectiv, acest lucru ar trebui să fie luat în considerare de Comisie înainte de a avea în vedere stabilirea unor specificații comune. Atunci când elaborează specificații comune, Comisia este încurajată să coopereze cu partenerii internaționali și cu organismele de standardizare internaționale.

- (122) Este oportun ca, fără a aduce atingere utilizării standardelor armonizate și a specificațiilor comune, să se prezume că furnizorii unui sistem de IA cu grad ridicat de risc care a fost antrenat și testat pe baza unor date care reflectă cadrul geografic, comportamental, contextual sau funcțional specific în care se intenționează utilizarea sistemului de IA respectă măsura relevantă prevăzută în temeiul cerinței privind guvernanta datelor stabilită în prezentul regulament. Fără a aduce atingere cerințelor legate de robustețe și acuratețe prevăzute în prezentul regulament, în conformitate cu articolul 54 alineatul (3) din Regulamentul (UE) 2019/881, ar trebui să se prezume că sistemele de IA cu grad ridicat de risc care au fost certificate sau pentru care a fost emisă o declarație de conformitate în cadrul unui sistem de securitate cibernetică în temeiul regulamentului respectiv, iar referințele aferente au fost publicate în *Jurnalul Oficial al Uniunii Europene*, respectă cerința de securitate cibernetică menționată în prezentul regulament, în măsura în care certificatul de securitate cibernetică sau declarația de conformitate sau părți ale acestora acoperă cerința de securitate cibernetică din prezentul regulament. Acest lucru nu aduce atingere caracterului voluntar al respectivului sistem de securitate cibernetică.
- (123) Pentru a asigura un nivel ridicat de fiabilitate a sistemelor de IA cu grad ridicat de risc, aceste sisteme ar trebui să facă obiectul unei evaluări a conformității înainte de introducerea lor pe piață sau de punerea lor în funcțiune.

- (124) Este oportun ca, pentru a reduce la minimum sarcina impusă operatorilor și pentru a evita eventualele suprapuneri, pentru sistemele de IA cu grad ridicat de risc legate de produse care fac obiectul legislației de armonizare existente a Uniunii bazate pe noul cadru legislativ, conformitatea acestor sisteme de IA cu cerințele prezentului regulament să fie evaluată ca parte a evaluării conformității prevăzute deja în legislația respectivă. Aplicabilitatea cerințelor prezentului regulament nu ar trebui, prin urmare, să afecteze logica specifică, metodologia sau structura generală a evaluării conformității în temeiul legislației de armonizare relevante a Uniunii.
- (125) Având în vedere complexitatea sistemelor de IA cu grad ridicat de risc și riscurile asociate acestora, este important să se dezvolte o procedură adecvată de evaluare a conformității pentru sistemele de IA cu grad ridicat de risc care implică organisme notificate, așa-numita evaluare a conformității de către terți. Cu toate acestea, având în vedere experiența actuală a organismelor profesionale de certificare înainte de introducerea pe piață în domeniul siguranței produselor și natura diferită a riscurilor implicate, este oportun să se limiteze, cel puțin într-o fază inițială de aplicare a prezentului regulament, domeniul de aplicare al evaluării conformității de către terți pentru sistemele de IA cu grad ridicat de risc, altele decât cele legate de produse. Prin urmare, evaluarea conformității unor astfel de sisteme ar trebui să fie efectuată, ca regulă generală, de către furnizor pe propria răspundere, cu singura excepție a sistemelor de IA destinate a fi utilizate pentru biometrie.

- (126) În vederea efectuării de evaluări ale conformității de către terți atunci când este necesar, autoritățile naționale competente ar trebui să comunice lista organismelor notificate în temeiul prezentului regulament, cu condiția ca acestea să îndeplinească un set de cerințe, în special în ceea ce privește independența, competența, absența conflictelor de interese și cerințele minime de securitate cibernetică. Lista acestor organisme notificate ar trebui să fie trimisă de autoritățile naționale competente Comisiei și celorlalte state membre prin intermediul instrumentului de notificare electronică dezvoltat și gestionat de Comisie în temeiul articolului R23 din anexa I la Decizia nr. 768/2008/CE.
- (127) În conformitate cu angajamentele asumate de Uniune în temeiul Acordului Organizației Mondiale a Comerțului privind barierele tehnice în calea comerțului, este adecvat să se faciliteze recunoașterea reciprocă a rezultatelor evaluării conformității obținute de organismele competente de evaluare a conformității, indiferent de teritoriul pe care sunt stabilite acestea, cu condiția ca respectivele organisme de evaluare a conformității instituite în temeiul dreptului unei țări terțe să îndeplinească cerințele aplicabile ale prezentului regulament, iar Uniunea să fi încheiat un acord în acest sens. În acest context, Comisia ar trebui să analizeze în mod activ posibile instrumente internaționale adecvate acestui scop și, în special, să urmărească încheierea de acorduri de recunoaștere reciprocă cu țări terțe.

- (128) În conformitate cu noțiunea stabilită de comun acord de modificare substanțială pentru produsele reglementate de legislația de armonizare a Uniunii, este oportun ca, ori de câte ori se produce o modificare care poate afecta respectarea prezentului regulament de către un sistem de IA cu grad ridicat de risc (de exemplu, modificarea sistemului de operare sau a arhitecturii software) sau atunci când scopul preconizat al sistemului se modifică, respectivul sistem de IA să fie considerat a fi un sistem de IA nou care ar trebui să facă obiectul unei noi evaluări a conformității. Cu toate acestea, modificările care afectează algoritmul și performanța sistemelor de IA care continuă să „învețe” după ce au fost introduse pe piață sau puse în funcțiune și anume, adaptarea automată a modului în care sunt îndeplinite funcțiile nu ar trebui să constituie o modificare substanțială, cu condiția ca modificările respective să fi fost prestabilite de furnizor și evaluate în momentul evaluării conformității.
- (129) Sistemele de IA cu grad ridicat de risc ar trebui să poarte marcajul CE pentru a indica conformitatea lor cu prezentul regulament, astfel încât să poată circula liber în cadrul pieței interne. Pentru sistemele de IA cu grad ridicat de risc încorporate într-un produs ar trebui să fie aplicat un marcaj CE fizic care poate fi completat de un marcaj CE digital. Pentru sistemele de IA cu grad ridicat de risc furnizate exclusiv digital, ar trebui să fie utilizat un marcaj CE digital. Statele membre ar trebui să nu genereze obstacole nejustificate în calea introducerii pe piață sau a punerii în funcțiune a sistemelor de IA cu grad ridicat de risc care sunt conforme cu cerințele prevăzute în prezentul regulament și care poartă marcajul CE.

- (130) În anumite condiții, disponibilitatea rapidă a tehnologiilor inovatoare poate fi esențială pentru sănătatea și siguranța persoanelor, pentru protecția mediului și combaterea schimbărilor climatice și pentru societate în ansamblu. Prin urmare, este oportun ca, din motive excepționale de siguranță publică sau de protecție a vieții și a sănătății persoanelor fizice, de protecție a mediului și de protecție a activelor industriale și de infrastructură esențiale, autoritățile de supraveghere a pieței să poată autoriza introducerea pe piață sau punerea în funcțiune a unor sisteme de IA care nu au fost supuse unei evaluări a conformității. În situații justificate în mod corespunzător, astfel cum se prevede în prezentul regulament, autoritățile de aplicare a legii sau autoritățile de protecție civilă pot pune în funcțiune un anumit sistem de IA cu grad ridicat de risc fără autorizarea autorității de supraveghere a pieței, cu condiția ca o astfel de autorizare să fie solicitată în timpul utilizării sau după utilizare, fără întârzieri nejustificate.
- (131) Pentru a facilita activitatea Comisiei și a statelor membre în domeniul IA, precum și pentru a spori transparența față de public, furnizorii de sisteme de IA cu grad ridicat de risc, altele decât cele legate de produse care intră în domeniul de aplicare al actelor legislative de armonizare relevante existente ale Uniunii, precum și furnizorii care consideră că un sistem de IA care figurează între situațiile cu grad ridicat de risc dintr-o anexă la prezentul regulament nu este, pe baza unei derogări, un sistem de IA cu grad ridicat de risc, ar trebui să aibă obligația de a se înregistra, precum și de a înregistra informații despre propriul sistem de IA într-o bază de date a UE, care urmează să fie creată și gestionată de Comisie. Înainte de a utiliza un sistem de IA care figurează între situațiile cu grad ridicat de risc dintr-o anexă la prezentul regulament, implementatorii sistemelor de IA cu grad ridicat de risc care sunt autorități, agenții sau organisme publice ar trebui să se înregistreze în baza de date respectivă și să selecteze sistemul pe care intenționează să îl utilizeze.

Ceilalți implementatori ar trebui să aibă dreptul de a face acest lucru în mod voluntar. Această secțiune a bazei de date a UE ar trebui să fie accesibilă publicului, în mod gratuit, informațiile ar trebui să fie ușor de parcurs, ușor de înțeles și prelucrabile automat. Baza de date a UE ar trebui, de asemenea, să fie ușor de utilizat, de exemplu prin furnizarea de funcționalități de căutare, inclusiv prin intermediul cuvintelor-cheie, care să permită publicului larg să găsească informațiile relevante care trebuie să fie transmise la înregistrarea sistemelor de IA cu grad ridicat de risc și cu privire la cazul de utilizare a sistemelor de IA cu grad ridicat de risc, prevăzute într-o anexă la prezentul regulament, cărora le corespund sistemele de IA cu grad ridicat de risc. Orice modificare substanțială a sistemelor de IA cu grad ridicat de risc ar trebui să se înregistreze, de asemenea, în baza de date a UE. Pentru sistemele de IA cu grad ridicat de risc din domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere, obligațiile de înregistrare ar trebui să fie îndeplinite în cadrul unei secțiuni securizate, care nu este accesibilă publicului, a bazei de date a UE. Accesul la secțiunea securizată care nu este accesibilă publicului ar trebui să fie strict limitat la Comisie, precum și la autoritățile de supraveghere a pieței în ceea ce privește secțiunea lor națională din baza de date respectivă. Sistemele de IA cu grad ridicat de risc din domeniul infrastructurii critice ar trebui să fie înregistrate exclusiv la nivel național. Comisia ar trebui să fie operatorul bazei de date a UE, în conformitate cu Regulamentul (UE) 2018/1725. Pentru a asigura funcționalitatea deplină a bazei de date a UE, atunci când aceasta este implementată, procedura de stabilire a bazei de date ar trebui să includă dezvoltarea de specificații funcționale de către Comisie și un raport de audit independent. Comisia ar trebui să țină seama de riscurile în materie de securitate cibernetică atunci când își îndeplinește sarcinile de operator de date în baza de date a UE. Pentru a maximiza disponibilitatea și utilizarea bazei de date a UE de către public, baza de date a UE, inclusiv informațiile puse la dispoziție prin intermediul acesteia, ar trebui să îndeplinească cerințele prevăzute în Directiva (UE) 2019/882.

- (132) Anumite sisteme de IA destinate să interacționeze cu persoane fizice sau să genereze conținut pot prezenta riscuri specifice de uzurpare a identității sau de înșelăciune, indiferent dacă acestea se califică drept sisteme cu grad ridicat de risc sau nu. Prin urmare, în anumite circumstanțe, utilizarea acestor sisteme ar trebui să facă obiectul unor obligații specifice în materie de transparență, fără a aduce atingere cerințelor și obligațiilor pentru sistemele de IA cu grad ridicat de risc și sub rezerva unor excepții specifice pentru a ține seama de nevoia specială de a aplica legea. În special, persoanele fizice ar trebui să fie informate că interacționează cu un sistem de IA, cu excepția cazului în care acest lucru este evident din punctul de vedere al unei persoane fizice rezonabil de bine informată, de atentă și de avizată, ținând seama de circumstanțele și contextul de utilizare. La punerea în aplicare a obligației respective, caracteristicile persoanelor fizice care aparțin grupurilor vulnerabile din motive de vârstă sau dizabilitate ar trebui să fie luate în considerare în măsura în care sistemul de IA este destinat să interacționeze și cu aceste grupuri. În plus, persoanele fizice ar trebui să fie informate atunci când sunt expuse la sisteme de IA care, prin prelucrarea datelor lor biometrice, pot identifica sau deduce emoțiile sau intențiile persoanelor respective sau le pot include în categorii specifice. Astfel de categorii specifice se pot referi la aspecte precum sexul, vârsta, culoarea părului, culoarea ochilor, tatuajele, trăsăturile personale, originea etnică, preferințele și interesele personale. Astfel de informații și notificări ar trebui să fie furnizate în formate accesibile pentru persoanele cu dizabilități.

(133) O varietate de sisteme de IA poate genera cantități mari de conținut sintetic, pe care oamenii ajung să îl distingă din ce în ce mai greu de conținutul autentic, generat de om. Disponibilitatea pe scară largă și capabilitățile din ce în ce mai mari ale acestor sisteme au un impact semnificativ asupra integrității ecosistemului informațional și a încrederii în acesta, generând noi riscuri de dezinformare și manipulare la scară largă, de fraudă, de uzurpare a identității și de inducere în eroare a consumatorilor. Având în vedere impactul respectiv, ritmul tehnologic rapid și necesitatea unor noi metode și tehnici de urmărire a originii informațiilor, este oportun să se solicite furnizorilor acestor sisteme să încorporeze soluții tehnice care să permită marcarea într-un format prelucrabil automat și detectarea faptului că rezultatul a fost generat sau manipulat de un sistem de IA, și nu de un om. Aceste tehnici și metode ar trebui să fie suficient de fiabile, interoperabile, eficace și robuste, în măsura în care acest lucru este fezabil din punct de vedere tehnic, ținând seama de tehnicile disponibile sau de o combinație de astfel de tehnici, cum ar fi filigrane, identificări prin intermediul metadatelor, metode criptografice pentru a dovedi proveniența și autenticitatea conținutului, metode de înregistrare, amprente digitale sau alte tehnici, după caz. Atunci când pun în aplicare această obligație, furnizorii ar trebui, de asemenea, să țină seama de particularitățile și limitările diferitelor tipuri de conținut și de evoluțiile tehnologice și ale pieței relevante în domeniu, astfel cum se reflectă în stadiul de avansare general recunoscut al tehnologiei. Astfel de tehnici și metode pot fi puse în aplicare la nivelul sistemului de IA sau la nivelul modelului de IA, inclusiv al modelelor de IA de uz general care generează conținut, facilitând astfel îndeplinirea acestei obligații de către furnizorul din aval al sistemului de IA. Este oportun să se aibă în vedere că, pentru a rămâne proporțională, această obligație de marcă nu ar trebui să vizeze sistemele de IA care îndeplinesc în principal o funcție de asistare pentru editarea standard sau sistemele de IA care nu modifică în mod substanțial datele de intrare furnizate de implementator sau semantica acestora.

- (134) Pe lângă soluțiile tehnice utilizate de furnizorii sistemului de IA, implementatorii care utilizează un sistem de IA pentru a genera sau a manipula conținuturi de imagine, audio sau video care se aseamănă în mod apreciabil cu persoane, obiecte, locuri, entități sau evenimente existente și care ar crea unei persoane impresia falsă că sunt autentice sau adevărate (deepfake-uri), ar trebui, de asemenea, să dezvăluie în mod clar și distinct faptul că respectivul conținut a fost creat sau manipulat în mod artificial prin etichetarea în consecință a rezultatului generat de IA și divulgarea originii sale artificiale. Respectarea acestei obligații de transparență nu ar trebui să fie interpretată în sensul de a indica că utilizarea sistemului de IA sau a rezultatelor sale împiedică dreptul la libertatea de exprimare și dreptul la libertatea artelor și științelor garantate de carte, în special atunci când conținutul face parte dintr-o lucrare sau dintr-un program în mod evident creativ, satiric, artistic, fictiv sau analog, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților. În cazurile respective, obligația de transparență pentru deepfake-uri prevăzută în prezentul regulament se limitează la divulgarea existenței unui astfel de conținut generat sau manipulat într-un mod adecvat, care să nu împiedice expunerea lucrării sau posibilitatea de a beneficia de aceasta, inclusiv exploatarea și utilizarea normală a acesteia, menținând în același timp utilitatea și calitatea lucrării. În plus, este, de asemenea, oportun să se aibă în vedere o obligație similară de divulgare în ceea ce privește textul generat sau manipulat de IA, în măsura în care acesta este publicat cu scopul de a informa publicul cu privire la chestiuni de interes public, cu excepția cazului în care conținutul generat de IA a fost supus unui proces de verificare editorială sau revizuire umană și responsabilitatea editorială pentru publicarea conținutului este deținută de o persoană fizică sau juridică.

- (135) Fără a aduce atingere caracterului obligatoriu și aplicabilității depline a obligațiilor privind transparența, Comisia poate, de asemenea, să încurajeze și să faciliteze elaborarea de coduri de bune practici la nivelul Uniunii cu scopul de a facilita punerea în aplicare efectivă a obligațiilor privind detectarea și etichetarea conținutului generat sau manipulat artificial, inclusiv de a sprijini modalitățile practice pentru a oferi accesul, după caz, la mecanisme de detectare și pentru a facilita cooperarea cu alți actori de-a lungul lanțului valoric, pentru a disemina conținutul sau a verifica autenticitatea și proveniența acestuia, astfel încât publicul să poată distinge efectiv conținutul generat de IA.
- (136) Obligațiile impuse prin prezentul regulament furnizorilor și implementatorilor anumitor sisteme de IA pentru a permite detectarea și divulgarea faptului că rezultatele sistemelor respective sunt generate sau manipulate artificial sunt deosebit de relevante pentru a facilita punerea în aplicare efectivă a Regulamentului (UE) 2022/2065. Acest lucru este valabil în special în ceea ce privește obligațiile furnizorilor de platforme online foarte mari sau de motoare de căutare online foarte mari de a identifica și a atenua riscurile sistemice care pot apărea în urma diseminării conținutului care a fost generat sau manipulat artificial, în special riscul privind efectele negative reale sau previzibile asupra proceselor democratice, asupra discursului civic și asupra proceselor electorale, inclusiv prin dezinformare. Cerința de etichetare a conținutului generat de sistemele de IA în temeiul prezentului regulament nu aduce atingere obligației prevăzute la articolul 16 alineatul (6) din Regulamentul (UE) 2022/2065 pentru furnizorii de servicii de găzduire de a prelucra notificările privind conținutul ilegal primite în temeiul articolului 16 alineatul (1) din regulamentul respectiv și nu ar trebui să influențeze evaluarea și decizia privind ilegalitatea conținutului specific. Evaluarea respectivă ar trebui să fie efectuată exclusiv în raport cu normele care reglementează legalitatea conținutului.

- (137) Respectarea obligațiilor privind transparența pentru sistemele de IA vizate de prezentul regulament nu ar trebui să fie interpretată ca indicând faptul că utilizarea sistemului de IA sau a rezultatelor sale este legală în temeiul prezentului regulament sau al altor dispoziții din dreptul Uniunii și al statelor membre și nu ar trebui să aducă atingere altor obligații de transparență pentru implementatorii sistemelor de IA prevăzute în dreptul Uniunii sau în cel intern.
- (138) IA este o familie de tehnologii care se dezvoltă rapid și care necesită supraveghere reglementară și un spațiu sigur și controlat pentru experimentare, asigurând, în același timp, inovarea responsabilă și integrarea unor garanții adecvate și a unor măsuri de atenuare a riscurilor. Pentru a asigura un cadru juridic care promovează inovarea, adaptat exigențelor viitorului și rezistent la inovări disruptive, statele membre ar trebui să se asigure că autoritățile lor naționale competente instituie cel puțin un spațiu de testare la nivel național în materie de reglementare în domeniul IA pentru a facilita dezvoltarea și testarea sistemelor de IA inovatoare aflate sub supraveghere reglementară strictă înainte ca aceste sisteme să fie introduse pe piață sau puse în funcțiune în alt mod. Statele membre ar putea, de asemenea, să îndeplinească această obligație prin participarea la spațiile de testare în materie de reglementare deja existente sau prin instituirea unui spațiu de testare în comun cu una sau mai multe autorități competente ale statelor membre, în măsura în care această participare asigură un nivel echivalent de acoperire națională pentru statele membre participante. Spațiile de testare în materie de reglementare în domeniul IA ar putea fi instituite în formă fizică, digitală sau hibridă și pot găzdui atât produse fizice, cât și produse digitale. Autoritățile de instituire ar trebui, de asemenea, să se asigure că spațiile de testare în materie de reglementare în domeniul IA dispun de resursele adecvate pentru funcționarea lor, inclusiv de resurse financiare și umane.

- (139) Obiectivele spațiilor de testare în materie de reglementare în domeniul IA ar trebui să fie promovarea inovării în domeniul IA prin instituirea unui mediu de experimentare și testare controlat în faza de dezvoltare și în faza anterioară introducerii pe piață, cu scopul de a asigura conformitatea sistemelor de IA inovatoare cu prezentul regulament și cu alte dispoziții relevante din dreptul Uniunii și dreptul intern. În plus, spațiile de testare în materie de reglementare în domeniul IA ar trebui să urmărească sporirea securității juridice pentru inovatori și supravegherea și înțelegerea de către autoritățile competente a oportunităților, a riscurilor emergente și a impactului utilizării IA, facilitarea învățării în materie de reglementare pentru autorități și întreprinderi, inclusiv în vederea viitoarelor adaptări ale cadrului juridic, sprijinirea cooperării și a schimbului de bune practici cu autoritățile implicate în spațiul de testare în materie de reglementare în domeniul IA, precum și accelerarea accesului la piețe, inclusiv prin eliminarea barierelor din calea IMM-urilor, inclusiv a întreprinderilor nou-înființate. Spațiile de testare în materie de reglementare în domeniul IA ar trebui să fie disponibile pe scară largă în întreaga Uniune și ar trebui să se acorde o atenție deosebită accesibilității acestora pentru IMM-uri, inclusiv pentru întreprinderile nou-înființate. Participarea la spațiul de testare în materie de reglementare în domeniul IA ar trebui să se concentreze pe aspecte care fac ca furnizorii și potențialii furnizori să se confrunte cu o lipsă de securitate juridică atunci când încearcă să inoveze, să experimenteze cu IA în Uniune și să contribuie la învățarea bazată pe dovezi în materie de reglementare. Supravegherea sistemelor de IA în spațiul de testare în materie de reglementare în domeniul IA ar trebui, prin urmare, să vizeze dezvoltarea, antrenarea, testarea și validarea acestora înainte ca sistemele să fie introduse pe piață sau puse în funcțiune, precum și noțiunea de modificare substanțială care ar putea necesita o nouă procedură de evaluare a conformității și ocurența unei astfel de modificări. Orice riscuri semnificative identificate în cursul dezvoltării și testării unor astfel de sisteme de IA ar trebui să conducă la o atenuare adecvată și, în cazul în care atenuarea nu este posibilă, la suspendarea procesului de dezvoltare și testare.

După caz, autoritățile naționale competente care instituie spații de testare în materie de reglementare în domeniul IA ar trebui să coopereze cu alte autorități relevante, inclusiv cu cele care supraveghează protecția drepturilor fundamentale, și ar putea permite implicarea altor actori din ecosistemul de IA, cum ar fi organizațiile de standardizare naționale sau europene, organismele notificate, unitățile de testare și experimentare, laboratoarele de cercetare și experimentare, centrele europene de inovare digitală și organizațiile relevante ale părților interesate și ale societății civile. Pentru a asigura o punere în aplicare uniformă în întreaga Uniune și economii de scară, este oportun să se stabilească norme comune pentru punerea în aplicare a spațiilor de testare în materie de reglementare în domeniul IA și un cadru de cooperare între autoritățile relevante implicate în supravegherea spațiilor de testare. Spațiile de testare în materie de reglementare în domeniul IA instituite în temeiul prezentului regulament nu ar trebui să aducă atingere altor dispoziții de drept care permit instituirea altor spații de testare cu scopul de a asigura conformitatea cu alte dispoziții de drept decât prezentul regulament. După caz, autoritățile competente relevante responsabile de aceste alte spații de testare în materie de reglementare ar trebui să ia în considerare beneficiile utilizării acestor spații de testare și în scopul asigurării conformității sistemelor de IA cu prezentul regulament. Pe baza unui acord între autoritățile naționale competente și participanții la spațiul de testare în materie de reglementare în domeniul IA, testarea în condiții reale poate fi, de asemenea, efectuată și supravegheată în cadrul spațiului de testare în materie de reglementare în domeniul IA.

- (140) Prezentul regulament ar trebui să ofere furnizorilor și potențialilor furnizori din cadrul spațiului de testare în materie de reglementare în domeniul IA temeiul juridic pentru utilizarea datelor cu caracter personal colectate în alte scopuri pentru a dezvolta anumite sisteme de IA de interes public în cadrul spațiului de testare în materie de reglementare în domeniul IA numai în condiții specificate, în conformitate cu articolul 6 alineatul (4) și cu articolul 9 alineatul (2) litera (g) din Regulamentul (UE) 2016/679, precum și cu articolele 5, 6 și 10 din Regulamentul (UE) 2018/1725 și fără a aduce atingere articolului 4 alineatul (2) și articolului 10 din Directiva (UE) 2016/680. Toate celelalte obligații ale operatorilor de date și drepturi ale persoanelor vizate în temeiul Regulamentelor (UE) 2016/679 și (UE) 2018/1725 și al Directivei (UE) 2016/680 rămân aplicabile. În special, prezentul regulament nu ar trebui să ofere un temei juridic în sensul articolului 22 alineatul (2) litera (b) din Regulamentul (UE) 2016/679 și al articolului 24 alineatul (2) litera (b) din Regulamentul (UE) 2018/1725. Furnizorii și potențialii furnizori din cadrul spațiului de testare în materie de reglementare în domeniul IA ar trebui să asigure garanții adecvate și să coopereze cu autoritățile competente, inclusiv urmând orientările acestora și acționând cu promptitudine și cu bună-credință, în ceea ce privește atenuarea în mod adecvat a oricăror riscuri semnificative identificate la adresa siguranței, sănătății și a drepturilor fundamentale care ar putea apărea în timpul dezvoltării, testării și experimentării în spațiul de testare respectiv.

- (141) Pentru a accelera procesul de dezvoltare și introducere pe piață a sistemelor de IA cu grad ridicat de risc enumerate într-o anexă la prezentul regulament, este important ca furnizorii sau potențialii furnizori ai acestor sisteme să poată beneficia, la rândul lor, de un regim specific pentru testarea acestor sisteme în condiții reale, fără a participa la un spațiu de testare în materie de reglementare în domeniul IA. Cu toate acestea, în astfel de cazuri, ținând seama de posibilele consecințe ale unor astfel de teste asupra persoanelor fizice, ar trebui să se garanteze faptul că prezentul regulament introduce garanții și condiții adecvate și suficiente pentru furnizori sau potențiali furnizori. Astfel de garanții ar trebui să includă, printre altele, solicitarea consimțământului în cunoștință de cauză al persoanelor fizice de a participa la teste în condiții reale, cu excepția cazurilor legate de aplicarea legii dacă solicitarea consimțământului în cunoștință de cauză ar împiedica testarea sistemului de IA. Consimțământul subiecților de a participa la astfel de teste în temeiul prezentului regulament este distinct de consimțământului persoanelor vizate pentru prelucrarea datelor lor cu caracter personal în temeiul dreptului relevant privind protecția datelor și nu îi aduce atingere acestuia.

De asemenea, este important să se reducă la minimum riscurile și să se permită supravegherea de către autoritățile competente și, prin urmare, să se impună potențialilor furnizori să facă demersurile necesare pentru prezentarea unui plan de testare în condiții reale autorității competente de supraveghere a pieței, să se înregistreze testările în secțiuni specifice din baza de date a UE, sub rezerva unor excepții limitate, să se instituie limite privind perioada pentru care se poate efectua testarea și să se impună garanții suplimentare pentru persoanele care aparțin anumitor grupuri vulnerabile, precum și un acord scris care să definească rolurile și responsabilitățile potențialilor furnizori și implementatori și supravegherea eficace de către personalul competent implicat în testarea în condiții reale. În plus, este oportun să se prevadă garanții suplimentare pentru a se asigura că previziunile, recomandările sau deciziile sistemului de IA pot fi efectiv inversate și ignorate și că datele cu caracter personal sunt protejate și sunt șterse atunci când subiecții își retrag consimțământul de a participa la testare, fără a aduce atingere drepturilor lor în calitate de persoane vizate în temeiul dreptului Uniunii privind protecția datelor. În ceea ce privește transferul de date, este, de asemenea, oportun să se prevadă că datele colectate și prelucrate în scopul testării în condiții reale ar trebui să fie transferate către țări terțe numai cu condiția punerii în aplicare a unor garanții adecvate și aplicabile în temeiul dreptului Uniunii, în special în conformitate cu bazele pentru transferul de date cu caracter personal în temeiul dreptului Uniunii privind protecția datelor, în timp ce pentru datele fără caracter personal sunt instituite garanții adecvate în conformitate cu dreptul Uniunii, cum ar fi Regulamentele (UE) 2022/868⁴² și (UE) 2023/2854⁴³ ale Parlamentului European și ale Consiliului.

⁴² Regulamentul (UE) 2022/868 al Parlamentului European și al Consiliului din 30 mai 2022 privind guvernarea datelor la nivel european și de modificare a Regulamentului (UE) 2018/1724 (Regulamentul privind guvernarea datelor) (JO L 152, 3.6.2022, p. 1).

⁴³ Regulamentul (UE) 2023/2854 al Parlamentului European și al Consiliului din 13 decembrie 2023 privind norme armonizate pentru un acces echitabil la date și o utilizare corectă a acestora și de modificare a Regulamentului (UE) 2017/2394 și a Directivei (UE) 2020/1828 (Regulamentul privind datele) (JO L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

- (142) Pentru a se asigura că IA conduce la rezultate benefice din punct de vedere social și ecologic, statele membre sunt încurajate să sprijine și să promoveze cercetarea și dezvoltarea de soluții de IA în sprijinul rezultatelor benefice din punct de vedere social și ecologic, cum ar fi soluțiile bazate pe IA pentru a spori accesibilitatea pentru persoanele cu dizabilități, pentru a combate inegalitățile socioeconomice sau pentru a îndeplini obiectivele de mediu, alocând resurse suficiente, inclusiv finanțare publică și din partea Uniunii, și, după caz și cu condiția îndeplinirii criteriilor de eligibilitate și de selecție, luând în considerare în special proiectele care urmăresc astfel de obiective. Aceste proiecte ar trebui să se bazeze pe principiul cooperării interdisciplinare dintre dezvoltatorii de IA, experții în materie de inegalitate și nediscriminare, accesibilitate, drepturile consumatorilor, de mediu și digitale, precum și cadrele universitare.

(143) Pentru a promova și proteja inovarea, este important să fie luate în considerare în mod deosebit interesele IMM-urilor, inclusiv ale întreprinderilor nou-înființate care sunt furnizori și implementatori de sisteme de IA. În acest scop, statele membre ar trebui să elaboreze inițiative care să vizeze operatorii respectivi, inclusiv în ceea ce privește sensibilizarea și comunicarea informațiilor. Statele membre ar trebui să ofere IMM-urilor, inclusiv întreprinderilor nou-înființate, care au un sediu social sau o sucursală în Uniune, acces prioritar la spațiile de testare în materie de reglementare în domeniul IA, cu condiția ca acestea să îndeplinească condițiile de eligibilitate și criteriile de selecție și fără a împiedica alți furnizori și potențiali furnizori să acceseze spațiile de testare, cu condiția să fie îndeplinite aceleași condiții și criterii. Statele membre ar trebui să utilizeze canalele existente și, după caz, să stabilească noi canale specifice de comunicare cu IMM-urile, inclusiv întreprinderile nou-înființate, implementatorii și alți inovatori și, după caz, cu autoritățile publice locale, pentru a sprijini IMM-urile pe tot parcursul dezvoltării lor, oferind orientări și răspunzând la întrebări cu privire la punerea în aplicare a prezentului regulament. După caz, aceste canale ar trebui să colaboreze pentru a crea sinergii și pentru a asigura omogenitatea orientărilor pe care le furnizează IMM-urilor, inclusiv întreprinderilor nou-înființate, și implementatorilor. În plus, statele membre ar trebui să faciliteze participarea IMM-urilor și a altor părți interesate relevante la procesele de elaborare a standardelor. De asemenea, ar trebui să fie luate în considerare interesele și nevoile specifice ale furnizorilor care sunt IMM-uri, inclusiv întreprinderi nou-înființate, atunci când organismele notificate stabilesc taxe de evaluare a conformității. Comisia ar trebui să evalueze periodic costurile de certificare și de conformitate suportate de IMM-uri, inclusiv de întreprinderile nou-înființate, prin consultări transparente și ar trebui să colaboreze cu statele membre pentru a reduce aceste costuri.

De exemplu, costurile de traducere legate de documentația obligatorie și de comunicarea cu autoritățile pot constitui un cost semnificativ pentru furnizori și alți operatori, în special pentru cei de dimensiuni mai mici. Statele membre ar trebui, eventual, să se asigure că una dintre limbile stabilite și acceptate pentru documentația relevantă din partea furnizorilor și pentru comunicarea cu operatorii este o limbă înțeleasă pe larg de un număr cât mai mare de implementatori transfrontalieri. Pentru a răspunde nevoilor specifice ale IMM-urilor, inclusiv ale întreprinderilor nou-înființate, Comisia ar trebui să furnizeze modele standardizate pentru domeniile vizate de prezentul regulament, la solicitarea Consiliului IA. În plus, Comisia ar trebui să completeze eforturile statelor membre prin furnizarea unei platforme unice de informare cu informații ușor de utilizat în ceea ce privește prezentul regulament destinate tuturor furnizorilor și implementatorilor, prin organizarea unor campanii de comunicare adecvate pentru sensibilizarea cu privire la obligațiile care decurg din prezentul regulament și prin evaluarea și promovarea convergenței bunelor practici în cadrul procedurilor de achiziții publice în ceea ce privește sistemele de IA. Întreprinderile mijlocii care până recent se încadrau în categoria de întreprinderi mici în sensul anexei la Recomandarea 2003/361/CE a Comisiei⁴⁴ ar trebui să aibă acces la măsurile de sprijin respective, deoarece este posibil ca aceste noi întreprinderi mijlocii să nu dispună uneori de resursele juridice și formarea necesare pentru a asigura respectarea și înțelegerea adecvată a prezentului regulament.

⁴⁴ Recomandarea Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii, (JO L 124, 20.5.2003, p. 36).

- (144) Pentru a promova și a proteja inovarea, platforma de IA la cerere și toate programele și proiectele de finanțare relevante ale Uniunii, cum ar fi programele Europa digitală și Orizont Europa, puse în aplicare de Comisie și de statele membre la nivelul Uniunii sau la nivel național, ar trebui, după caz, să contribuie la îndeplinirea obiectivelor prezentului regulament.
- (145) Pentru a reduce la minimum riscurile la adresa punerii în aplicare care decurg din lipsa de cunoaștere și de cunoștințe de specialitate de pe piață, precum și pentru a facilita respectarea de către furnizori, cu precădere de către IMM-uri, inclusiv întreprinderile nou-înființate, precum și de către organismele notificate a obligațiilor care le revin în temeiul prezentului regulament, platforma de IA la cerere, centrele europene de inovare digitală și instalațiile de testare și experimentare instituite de Comisie și de statele membre la nivelul Uniunii sau la nivel național ar trebui să contribuie la punerea în aplicare a prezentului regulament. În cadrul misiunii și domeniilor lor de competență respective, platforma de IA la cerere, centrele europene de inovare digitală și instalațiile de testare și experimentare sunt în măsură să ofere, în special, sprijin tehnic și științific furnizorilor și organismelor notificate.

- (146) În plus, având în vedere dimensiunea foarte mică a unor operatori și pentru a asigura proporționalitatea în ceea ce privește costurile inovării, este oportun să se permită microîntreprinderilor să îndeplinească într-o manieră simplificată una dintre obligațiile cele mai costisitoare, și anume aceea de a institui un sistem de management al calității, fapt care ar reduce sarcina administrativă și costurile pentru întreprinderile respective, fără a afecta nivelul de protecție și necesitatea de a respecta cerințele pentru sistemele de IA cu grad ridicat de risc. Comisia ar trebui să elaboreze orientări pentru a specifica elementele sistemului de management al calității care trebuie îndeplinite în această manieră simplificată de către microîntreprinderi.
- (147) Este oportun ca, în măsura posibilului, Comisia să faciliteze accesul la instalațiile de testare și experimentare pentru organisme, grupurile sau laboratoarele înființate sau acreditate în temeiul oricăror acte legislative de armonizare relevante ale Uniunii și care îndeplinesc sarcini în contextul evaluării conformității produselor sau dispozitivelor reglementate de respectivele acte legislative de armonizare ale Uniunii. Acest lucru este valabil în special în ceea ce privește grupurile de experți, laboratoarele de expertiză și laboratoarele de referință în domeniul dispozitivelor medicale în temeiul Regulamentelor (UE) 2017/745 și (UE) 2017/746.

(148) Prezentul regulament ar trebui să instituie un cadru de guvernanță care să permită, pe de o parte, coordonarea și sprijinirea aplicării prezentului regulament la nivel național și, pe de altă parte, consolidarea capabilităților la nivelul Uniunii și integrarea părților interesate în domeniul IA. Punerea în aplicare și respectarea efectivă a prezentului regulament necesită un cadru de guvernanță care să permită coordonarea și consolidarea cunoștințelor de specialitate centrale la nivelul Uniunii. Oficiul pentru IA a fost instituit printr-o decizie a Comisiei⁴⁵ și are ca misiune să dezvolte cunoștințele de specialitate și capabilitățile Uniunii în domeniul IA și să contribuie la punerea în aplicare a dreptului Uniunii privind IA. Statele membre ar trebui să faciliteze sarcinile Oficiului pentru IA cu scopul de a sprijini dezvoltarea, la nivelul Uniunii, a cunoștințelor de specialitate și a capabilităților Uniunii și de a consolida funcționarea pieței unice digitale. În plus, ar trebui să fie instituit un Consiliu IA compus din reprezentanți ai statelor membre, un grup științific care să integreze comunitatea științifică și un forum consultativ pentru a furniza contribuții ale părților interesate pentru punerea în aplicare a prezentului regulament, la nivelul Uniunii și la nivel național. Dezvoltarea cunoștințelor de specialitate și a capabilităților Uniunii ar trebui să includă și valorificarea resurselor și cunoștințelor de specialitate existente, în special prin sinergii cu structurile create în contextul aplicării la nivelul Uniunii a altor acte legislative și al sinergiilor cu inițiativele conexe de la nivelul Uniunii, cum ar fi Întreprinderea comună EuroHPC și unitățile de testare și experimentare în domeniul IA din cadrul programului „Europa digitală”.

⁴⁵ Decizia Comisiei din 24.1.2024 de instituire a Oficiului european pentru inteligența artificială, C(2024) 390.

(149) Pentru a facilita o punere în aplicare armonioasă, efectivă și armonizată a prezentului regulament, ar trebui să fie instituit un Consiliu IA. Consiliul IA ar trebui să reflecte diferitele interese ale ecosistemului de IA și să fie alcătuit din reprezentanți ai statelor membre. Consiliul IA ar trebui să fie responsabil pentru o serie de sarcini consultative, inclusiv emiterea de avize, recomandări, consiliere sau furnizarea unor contribuții sub formă de orientări cu privire la aspecte legate de punerea în aplicare a prezentului regulament, inclusiv cu privire la aspecte de aplicare a legii, la specificații tehnice sau la standarde existente în ceea ce privește cerințele stabilite în prezentul regulament, precum și furnizarea de consiliere Comisiei și statelor lor membre și autorităților naționale competente ale acestora cu privire la chestiuni specifice legate de IA. Pentru a oferi o anumită flexibilitate statelor membre în ceea ce privește desemnarea reprezentanților lor în cadrul Consiliului IA, astfel de reprezentanți pot fi persoane care aparțin unor entități publice care ar trebui să aibă competențele și prerogativele relevante pentru a facilita coordonarea la nivel național și pentru a contribui la îndeplinirea sarcinilor Consiliului IA. Consiliul IA ar trebui să instituie două subgrupuri permanente pentru a oferi o platformă de cooperare și de schimb între autoritățile de supraveghere a pieței și autoritățile de notificare cu privire la aspecte legate de supravegherea pieței și, respectiv, de organismele notificate. Subgrupul permanent pentru supravegherea pieței ar trebui să acționeze în calitate de grup de cooperare administrativă (ADCO) pentru prezentul regulament în sensul articolului 30 din Regulamentul (UE) 2019/1020. În conformitate cu articolul 33 din regulamentul respectiv, Comisia ar trebui să sprijine activitățile subgrupului permanent pentru supravegherea pieței prin efectuarea de evaluări sau studii de piață, în special în vederea identificării aspectelor prezentului regulament care necesită o coordonare specifică și urgentă între autoritățile de supraveghere a pieței. Consiliul IA poate înființa alte subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice. Consiliul IA ar trebui, de asemenea, să coopereze, după caz, cu organismele, grupurile de experți și rețelele relevante ale Uniunii care își desfășoară activitatea în contextul reglementărilor relevante ale dreptului Uniunii, inclusiv, în special, cu cele care își desfășoară activitatea în temeiul reglementărilor relevante ale dreptului Uniunii privind datele, produsele și serviciile digitale.

- (150) Pentru a asigura implicarea părților interesate în punerea în aplicare și aplicarea prezentului regulament, ar trebui să fie instituit un forum consultativ care să furnizeze Consiliului IA și Comisiei consiliere și cunoștințe de specialitate tehnice. Pentru a asigura o reprezentare a părților interesate variată și echilibrată între interesele comerciale și cele necomerciale și, în cadrul categoriei intereselor comerciale, în ceea ce privește IMM-urile și alte întreprinderi, forumul consultativ ar trebui să cuprindă, printre altele, industria, întreprinderile nou-înființate, IMM-urile, mediul academic, societatea civilă, inclusiv partenerii sociali, precum și Agenția pentru Drepturi Fundamentale, ENISA, Comitetul European de Standardizare (CEN), Comitetul European de Standardizare în Electrotehnică (CENELEC) și Institutul European de Standardizare în Telecomunicații (ETSI).
- (151) Pentru a sprijini punerea în aplicare și respectarea prezentului regulament, în special activitățile de monitorizare ale Oficiului pentru IA în ceea ce privește modelele de IA de uz general, ar trebui să fie instituit un grup științific de experți independenți. Experții independenți din alcătuirea grupului științific ar trebui să fie selectați pe baza cunoștințelor de specialitate științifice sau tehnice actualizate în domeniul IA și ar trebui să își îndeplinească sarcinile cu imparțialitate și obiectivitate și să asigure confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și activităților lor. Pentru a permite consolidarea capacităților naționale necesare pentru aplicarea efectivă a prezentului regulament, statele membre ar trebui să poată solicita sprijin echipei de experți care formează grupul științific pentru activitățile lor de aplicare a legii.

- (152) Pentru a sprijini o aplicare adecvată a normelor în ceea ce privește sistemele de IA și pentru a consolida capacitățile statelor membre, ar trebui să fie instituite și puse la dispoziția statelor membre structuri ale Uniunii de sprijin pentru testarea IA.
- (153) Statele membre joacă un rol esențial în aplicarea și respectarea prezentului regulament. În acest sens, fiecare stat membru ar trebui să desemneze cel puțin o autoritate de notificare și cel puțin o autoritate de supraveghere a pieței în calitatea de autorități naționale competente în scopul supravegherii aplicării și punerii în aplicare a prezentului regulament. Statele membre pot decide să numească orice tip de entitate publică pentru a îndeplini sarcinile autorităților naționale competente în sensul prezentului regulament, în conformitate cu caracteristicile și nevoile organizaționale naționale specifice ale acestora. Pentru a spori eficiența organizațională din partea statelor membre și pentru a stabili un punct unic de contact cu publicul și cu alți omologi la nivelul statelor membre și al Uniunii, fiecare stat membru ar trebui să desemneze o autoritate de supraveghere a pieței care să acționeze ca punct unic de contact.
- (154) Autoritățile naționale competente ar trebui să își exercite competențele în mod independent, imparțial și fără prejudecăți, garantând principiile obiectivității activităților și sarcinilor lor și asigurând aplicarea și punerea în aplicare a prezentului regulament. Membrii acestor autorități ar trebui să se abțină de la orice act incompatibil cu natura funcțiilor lor și ar trebui să facă obiectul normelor de confidențialitate în temeiul prezentului regulament.

- (155) Pentru a se asigura că furnizorii de sisteme de IA cu grad ridicat de risc pot ține seama de experiența privind utilizarea sistemelor de IA cu grad ridicat de risc pentru îmbunătățirea sistemelor lor și a procesului de proiectare și dezvoltare sau că pot lua orice măsură corectivă posibilă în timp util, toți furnizorii ar trebui să dispună de un sistem de monitorizare ulterioară introducerii pe piață. După caz, monitorizarea ulterioară introducerii pe piață ar trebui să includă o analiză a interacțiunii cu alte sisteme de IA, inclusiv cu alte dispozitive și alt software. Monitorizarea ulterioară introducerii pe piață nu ar trebui să vizeze datele operaționale sensibile ale implementatorilor care sunt autorități de aplicare a legii. Acest sistem este, de asemenea, esențial pentru a se asigura că posibilele riscuri care decurg din sistemele de IA care continuă să „învețe” după ce au fost introduse pe piață sau puse în funcțiune pot fi abordate într-un mod mai eficient și în timp util. În acest context, furnizorii ar trebui, de asemenea, să aibă obligația de a dispune de un sistem pentru a raporta autorităților relevante orice incident grav care decurge din utilizarea sistemelor lor de IA, și anume un incident sau o funcționare defectuoasă care duce la deces sau la daune grave pentru sănătate, la perturbări grave și ireversibile ale gestionării și funcționării infrastructurii critice, la încălcări ale obligațiilor în temeiul dreptului Uniunii menite să protejeze drepturile fundamentale sau la daune grave aduse bunurilor materiale sau mediului.

(156) Pentru a se asigura respectarea adecvată și efectivă a cerințelor și a obligațiilor prevăzute în prezentul regulament, și anume în legislația de armonizare a Uniunii, ar trebui să se aplice sistemul de supraveghere a pieței și de conformitate a produselor în ansamblul său, astfel cum a fost instituit prin Regulamentul (UE) 2019/1020. Autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament ar trebui să dispună de toate competențele de aplicare a dispozițiilor stabilite în prezentul regulament și în Regulamentul (UE) 2019/1020 și ar trebui să își exercite competențele și să își îndeplinească atribuțiile în mod independent, imparțial și fără prejudecăți. Deși majoritatea sistemelor de IA nu fac obiectul unor cerințe și obligații specifice în temeiul prezentului regulament, autoritățile de supraveghere a pieței pot lua măsuri în legătură cu toate sistemele de IA atunci când acestea prezintă un risc în conformitate cu prezentul regulament. Având în vedere natura specifică a instituțiilor, agențiilor și organelor Uniunii care intră în domeniul de aplicare al prezentului regulament, este oportun ca Autoritatea Europeană pentru Protecția Datelor să fie desemnată drept autoritate competentă de supraveghere a pieței pentru acestea. Acest lucru nu ar trebui să aducă atingere desemnării autorităților naționale competente de către statele membre. Activitățile de supraveghere a pieței nu ar trebui să afecteze capacitatea entităților supravegheate de a-și îndeplini sarcinile în mod independent, atunci când independența lor este impusă de dreptul Uniunii.

(157) Prezentul regulament nu aduce atingere competențelor, sarcinilor, prerogativelor și independenței autorităților sau organismelor publice naționale relevante care supraveghează aplicarea dreptului Uniunii care protejează drepturile fundamentale, inclusiv ale organismelor de promovare a egalității și ale autorităților de protecție a datelor. În cazul în care acest lucru este necesar pentru îndeplinirea mandatului lor, autoritățile sau organismele publice naționale respective ar trebui să aibă, de asemenea, acces la orice documentație creată în temeiul prezentului regulament. Ar trebui să fie stabilită o procedură de salvagardare specifică pentru a se asigura respectarea dispozițiilor în domeniul IA, în mod adecvat și în timp util, în privința sistemelor de IA care prezintă un risc pentru sănătate, siguranță și drepturile fundamentale. Procedura pentru astfel de sisteme de IA care prezintă un risc ar trebui să se aplice sistemelor de IA cu grad ridicat de risc care prezintă un risc, sistemelor interzise care au fost introduse pe piață, puse în funcțiune sau utilizate cu încălcarea interdicției anumitor practici prevăzută în prezentul regulament, precum și sistemelor de IA care au fost puse la dispoziție cu încălcarea cerințelor de transparență prevăzute în prezentul regulament și care prezintă un risc.

- (158) Dreptul Uniunii privind serviciile financiare include norme și cerințe privind guvernanta internă și gestionarea riscurilor care sunt aplicabile instituțiilor financiare reglementate în cursul furnizării acestor servicii, inclusiv atunci când acestea utilizează sisteme de IA. Pentru a asigura, în mod coerent, aplicarea și respectarea obligațiilor prevăzute în prezentul regulament și a normelor și cerințelor relevante ale actelor juridice ale Uniunii în domeniul serviciilor financiare, autoritățile competente responsabile cu supravegherea și aplicarea actelor juridice respective, în special autoritățile competente, astfel cum sunt definite în Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului⁴⁶ și în Directivele 2008/48/CE⁴⁷, 2009/138/CE⁴⁸, 2013/36/UE⁴⁹, 2014/17/UE⁵⁰ și (UE) 2016/97⁵¹ ale Parlamentului European și ale Consiliului, ar trebui să fie desemnate, în limitele competențelor lor respective, drept autorități competente în scopul supravegherii punerii în aplicare a prezentului regulament, inclusiv pentru activitățile de supraveghere a pieței, în ceea ce privește sistemele de IA furnizate sau utilizate de instituțiile financiare reglementate și supravegheate, cu excepția cazului în care statele membre decid să desemneze o altă autoritate pentru a îndeplini aceste sarcini de supraveghere a pieței.

⁴⁶ Regulamentul (UE) nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și societățile de investiții și de modificare a Regulamentului (UE) nr. 648/2012 (JO L 176, 27.6.2013, p. 1).

⁴⁷ Directiva 2008/48/CE a Parlamentului European și a Consiliului din 23 aprilie 2008 privind contractele de credit pentru consumatori și de abrogare a Directivei 87/102/CEE a Consiliului (JO L 133, 22.5.2008, p. 66).

⁴⁸ Directiva 2009/138/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 privind accesul la activitate și desfășurarea activității de asigurare și de reasigurare (Solvabilitate II) (JO L 335, 17.12.2009, p. 1).

⁴⁹ Directiva 2013/36/UE a Parlamentului European și a Consiliului din 26 iunie 2013 cu privire la accesul la activitatea instituțiilor de credit și supravegherea prudențială a instituțiilor de credit și a firmelor de investiții, de modificare a Directivei 2002/87/CE și de abrogare a Directivelor 2006/48/CE și 2006/49/CE (JO L 176, 27.6.2013, p. 338).

⁵⁰ Directiva 2014/17/UE a Parlamentului European și a Consiliului din 4 februarie 2014 privind contractele de credit oferite consumatorilor pentru bunuri imobile rezidențiale și de modificare a Directivelor 2008/48/CE și 2013/36/UE și a Regulamentului (UE) nr. 1093/2010 (JO L 60, 28.2.2014, p. 34).

⁵¹ Directiva (UE) 2016/97 a Parlamentului European și a Consiliului din 20 ianuarie 2016 privind distribuția de asigurări (JO L 26, 2.2.2016, p. 19).

Autoritățile competente respective ar trebui să dețină toate competențele în temeiul prezentului regulament și al Regulamentului (UE) 2019/1020 pentru a asigura respectarea cerințelor și a obligațiilor prevăzute în prezentul regulament, inclusiv competențele de a desfășura activități **ex post** de supraveghere a pieței care pot fi integrate, după caz, în mecanismele și procedurile lor de supraveghere existente în temeiul dispozițiilor relevante ale dreptului Uniunii din domeniul serviciilor financiare. Este oportun să se considere că, atunci când acționează în calitate de autorități de supraveghere a pieței în temeiul prezentului regulament, autoritățile naționale responsabile de supravegherea instituțiilor de credit reglementate în temeiul Directivei 2013/36/UE, care participă la mecanismul unic de supraveghere instituit prin Regulamentul (UE) nr. 1024/2013 al Consiliului⁵², ar trebui să raporteze fără întârziere Băncii Centrale Europene orice informații identificate în cursul activităților lor de supraveghere a pieței care ar putea prezenta un interes pentru sarcinile de supraveghere prudențială ale Băncii Centrale Europene, astfel cum se specifică în regulamentul respectiv. Pentru a spori și mai mult coerența dintre prezentul regulament și normele aplicabile instituțiilor de credit reglementate în temeiul Directivei 2013/36/UE, este, de asemenea, oportun să se integreze unele dintre obligațiile procedurale ale furnizorilor în ceea ce privește gestionarea riscurilor, monitorizarea ulterioară introducerii pe piață și documentația în obligațiile și procedurile existente în temeiul Directivei 2013/36/UE. Pentru a evita suprapunerile, ar trebui să fie avute în vedere derogări limitate și în ceea ce privește sistemul de management al calității al furnizorilor și obligația de monitorizare impusă implementatorilor de sisteme de IA cu grad ridicat de risc, în măsura în care acestea se aplică instituțiilor de credit reglementate de Directiva 2013/36/UE. Același regim ar trebui să se aplice întreprinderilor de asigurare și reasigurare și holdingurilor de asigurare în temeiul Directivei 2009/138/CE, intermediarilor de asigurări în temeiul Directivei (UE) 2016/97, precum și altor tipuri de instituții financiare care fac obiectul cerințelor privind guvernanța internă, măsurile sau procesele interne instituite în temeiul dispozițiilor relevante ale dreptului Uniunii din domeniul serviciilor financiare pentru a asigura coerența și egalitatea de tratament în sectorul financiar.

⁵² Regulamentul (UE) nr. 1024/2013 al Consiliului din 15 octombrie 2013 de conferire a unor atribuții specifice Băncii Centrale Europene în ceea ce privește politicile legate de supravegherea prudențială a instituțiilor de credit (JO L 287, 29.10.2013, p. 63).

- (159) Fiecare autoritate de supraveghere a pieței pentru sistemele de IA cu grad ridicat de risc din domeniul biometriei, astfel cum sunt enumerate într-o anexă la prezentul regulament, în măsura în care sistemele respective sunt utilizate în scopul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere sau al administrării justiției și al proceselor democratice, ar trebui să aibă competențe de investigare și corective efective, inclusiv cel puțin competența de a obține acces la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale. Autoritățile de supraveghere a pieței ar trebui să își poată exercita competențele acționând cu deplină independență. Nicio limitare a accesului acestora la date operaționale sensibile în temeiul prezentului regulament nu ar trebui să aducă atingere competențelor care le sunt conferite prin Directiva (UE) 2016/680. Nicio excludere în ceea ce privește divulgarea de date către autoritățile naționale de protecție a datelor în temeiul prezentului regulament nu ar trebui să afecteze competențele actuale sau viitoare ale autorităților respective în afara domeniului de aplicare al prezentului regulament.
- (160) Autoritățile de supraveghere a pieței și Comisia ar trebui să poată propune activități comune, inclusiv investigații comune, care să fie efectuate de autoritățile de supraveghere a pieței sau de autoritățile de supraveghere a pieței în colaborare cu Comisia și care au scopul de a promova conformitatea, de a identifica cazurile de neconformitate, de a sensibiliza și de a oferi orientări în legătură cu prezentul regulament în ceea ce privește anumite categorii de sisteme de IA cu grad ridicat de risc despre care se constată că prezintă un risc grav în două sau mai multe state membre. Activitățile comune de promovare a conformității ar trebui desfășurate în conformitate cu articolul 9 din Regulamentul (UE) 2019/1020. Oficiul pentru IA ar trebui să ofere sprijin sub formă de coordonare pentru investigațiile comune.

- (161) Este necesar să se clarifice responsabilitățile și competențele la nivelul Uniunii și la nivel național în ceea ce privește sistemele de IA care au la bază modele de IA de uz general. Pentru a evita suprapunerea competențelor, în cazul în care un sistem de IA se bazează pe un model de IA de uz general, iar modelul și sistemul sunt furnizate de același furnizor, supravegherea ar trebui să aibă loc la nivelul Uniunii prin intermediul Oficiului pentru IA, care, în acest scop, ar trebui să dețină competențele unei autorități de supraveghere a pieței în sensul Regulamentului (UE) 2019/1020. În toate celelalte cazuri, responsabilitatea privind supravegherea sistemelor de IA rămâne în sarcina autorităților naționale de supraveghere a pieței. Cu toate acestea, pentru sistemele de IA de uz general care pot fi utilizate direct de către implementatori pentru cel puțin un scop clasificat ca prezentând un grad ridicat de risc, autoritățile de supraveghere a pieței ar trebui să coopereze cu Oficiul pentru IA pentru a efectua evaluări ale conformității și să informeze în consecință Consiliul IA și alte autorități de supraveghere a pieței. În plus, autoritățile de supraveghere a pieței ar trebui să poată solicita asistență din partea Oficiului pentru IA în cazul în care autoritatea de supraveghere a pieței nu este în măsură să finalizeze o investigație cu privire la un sistem de IA cu grad ridicat de risc din cauza incapacității sale de a accesa anumite informații legate de modelul de IA de uz general care stă la baza sistemului de IA cu grad ridicat de risc. În astfel de cazuri, ar trebui să se aplice *mutatis mutandis* procedura privind asistența reciprocă transfrontalieră din capitolul VI din Regulamentul (UE) 2019/1020.

- (162) Pentru a utiliza în mod optim cunoștințele de specialitate centralizate ale Uniunii și sinergiile de la nivelul Uniunii, competențele de supraveghere și de executare a obligațiilor care le revin furnizorilor de modele de IA de uz general ar trebui să fie deținute de Comisie. Oficiul pentru IA ar trebui să fie în măsură să întreprindă toate acțiunile necesare pentru a monitoriza punerea în aplicare efectivă a prezentului regulament în ceea ce privește modelele de IA de uz general. Acesta ar trebui să fie în măsură să investigheze posibilele încălcări ale normelor privind furnizorii de modele de IA de uz general, atât din proprie inițiativă, dând curs rezultatelor activităților sale de monitorizare, cât și la cererea autorităților de supraveghere a pieței, în conformitate cu condițiile stabilite în prezentul regulament. Pentru a sprijini desfășurarea în mod eficace de către Oficiul pentru IA a monitorizării, acesta ar trebui să prevadă posibilitatea ca furnizorii din aval să depună plângeri cu privire la posibile încălcări ale normelor privind furnizorii de sisteme și modele de IA de uz general.
- (163) În vederea completării sistemelor de guvernanță pentru modelele de IA de uz general, grupul științific ar trebui să sprijine activitățile de monitorizare ale Oficiului pentru IA și poate, în anumite cazuri, să furnizeze Oficiului pentru IA alerte calificate care declanșează acțiuni subsecvente, de exemplu investigații. Acest lucru ar trebui să fie valabil atunci când grupul științific are motive să suspecteze că un model de IA de uz general prezintă un risc concret și identificabil la nivelul Uniunii. În plus, acest lucru ar trebui să fie valabil atunci când grupul științific are motive să suspecteze că un model de IA de uz general îndeplinește criteriile care ar conduce la o clasificare ca model de IA de uz general cu risc sistemic. Pentru ca grupul științific să dispună de informațiile necesare în îndeplinirea sarcinilor respective, ar trebui să existe un mecanism prin care acesta să poată solicita Comisiei să impună furnizorilor să ofere documente sau informații.

- (164) Oficiul pentru IA ar trebui să poată lua măsurile necesare pentru a monitoriza punerea în aplicare efectivă și respectarea obligațiilor furnizorilor de modele de IA de uz general prevăzute în prezentul regulament. Oficiul pentru IA ar trebui să fie în măsură să investigheze posibilele încălcări în conformitate cu competențele prevăzute în prezentul regulament, inclusiv prin solicitarea unor documente și informații, prin desfășurarea de evaluări, precum și prin solicitarea luării de măsuri de către furnizorii de modele de IA de uz general. În desfășurarea evaluărilor, pentru a utiliza cunoștințe de specialitate cu caracter independent, Oficiul pentru IA ar trebui să poată implica experți independenți pentru a desfășura evaluările în numele său. Respectarea obligațiilor ar trebui să fie asigurată, printre altele, prin cereri de a lua măsuri adecvate, inclusiv măsuri de atenuare a riscurilor în cazul unor riscuri sistemice identificate, precum și prin restricționarea punerii la dispoziție pe piață, retragerea sau rechemarea modelului. Ca o garanție, în cazul în care aceasta este necesară dincolo de drepturile procedurale prevăzute în prezentul regulament, furnizorii de modele de IA de uz general ar trebui să beneficieze de drepturile procedurale prevăzute la articolul 18 din Regulamentul (UE) 2019/1020, care ar trebui să se aplice *mutatis mutandis*, fără a aduce atingere drepturilor procedurale mai specifice prevăzute în prezentul regulament.

(165) Dezvoltarea altor sisteme de IA decât cele cu grad ridicat de risc în conformitate cu cerințele prezentului regulament poate duce la o utilizare pe scară mai largă a IA conform unor principii etice și fiabile în Uniune. Furnizorii de sisteme de IA care nu prezintă un grad ridicat de risc ar trebui să fie încurajați să creeze coduri de conduită, inclusiv mecanisme de guvernare conexe, menite să promoveze aplicarea parțială sau integrală, în mod voluntar, a cerințelor obligatorii aplicabile sistemelor de IA cu grad ridicat de risc, adaptate în funcție de scopul preconizat al sistemelor și de riscul mai scăzut implicat și ținând seama de soluțiile tehnice disponibile și de bunele practici din industrie, cum ar fi modelele și cardurile de date. Furnizorii și, după caz, implementatorii tuturor modelelor de IA și sistemelor de IA cu sau fără grad ridicat de risc ar trebui, de asemenea, să fie încurajați să aplice în mod voluntar cerințe suplimentare legate, de exemplu, de elementele Orientărilor Uniunii în materie de etică pentru o IA fiabilă, de durabilitatea mediului, de măsuri de alfabetizare în domeniul IA, de proiectarea și dezvoltarea sistemelor de IA ținând seama de incluziune și diversitate, inclusiv acordând atenție persoanelor vulnerabile și accesibilității pentru persoanele cu dizabilități, de participarea părților interesate în proiectarea și dezvoltarea sistemelor de IA, cu implicarea, după caz, a părților interesate relevante, cum ar fi întreprinderi și organizații ale societății civile, mediul academic, organizații de cercetare, sindicate și organizații de protecție a consumatorilor, precum și de diversitatea în cadrul echipelor de dezvoltare, inclusiv echilibrul de gen. Pentru a se asigura eficacitatea lor, codurile de conduită voluntare ar trebui să se bazeze pe obiective clare și pe indicatori-cheie de performanță pentru a măsura îndeplinirea obiectivelor respective. Acestea ar trebui, de asemenea, să fie dezvoltate într-un mod incluziv, după caz, cu implicarea părților interesate relevante, cum ar fi întreprinderi și organizații ale societății civile, mediul academic, organizații de cercetare, sindicate și organizații de protecție a consumatorilor. Comisia poate elabora inițiative, inclusiv de natură sectorială, pentru a facilita reducerea barierelor tehnice care împiedică schimbul transfrontalier de date pentru dezvoltarea IA, inclusiv în ceea ce privește infrastructura de acces la date și interoperabilitatea semantică și tehnică a diferitelor tipuri de date.

- (166) Este important ca sistemele de IA legate de produse care nu prezintă un risc ridicat în conformitate cu prezentul regulament și care, prin urmare, nu sunt obligate să respecte cerințele prevăzute pentru sistemele de IA cu grad ridicat de risc să fie totuși sigure atunci când sunt introduse pe piață sau puse în funcțiune. Pentru a contribui la acest obiectiv, Regulamentul (UE) 2023/988 al Parlamentului European și a Consiliului⁵³ ar fi aplicat ca o „plasă de siguranță”.
- (167) Pentru a asigura o cooperare de încredere și constructivă a autorităților competente la nivelul Uniunii și la nivel național, toate părțile implicate în aplicarea prezentului regulament ar trebui să respecte confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor lor, în conformitate cu dreptul Uniunii sau cu dreptul intern. Acestea ar trebui să își îndeplinească sarcinile și activitățile astfel încât să protejeze, în special, drepturile de proprietate intelectuală, informațiile comerciale confidențiale și secretele comerciale, punerea în aplicare efectivă a prezentului regulament, interesele de securitate publică și națională, integritatea procedurilor penale și administrative și integritatea informațiilor clasificate.

⁵³ Regulamentul (UE) 2023/988 al Parlamentului European și al Consiliului din 10 mai 2023 privind siguranța generală a produselor, de modificare a Regulamentului (UE) nr. 1025/2012 al Parlamentului European și al Consiliului și a Directivei (UE) 2020/1828 a Parlamentului European și a Consiliului și de abrogare a Directivei 2001/95/CE a Parlamentului European și a Consiliului și a Directivei 87/357/CEE a Consiliului (JO L 135, 23.5.2023, p. 1).

- (168) Respectarea prezentului regulament ar trebui să fie asigurată prin impunerea de sancțiuni și alte măsuri de executare. Statele membre ar trebui să ia toate măsurile necesare pentru a se asigura că sunt puse în aplicare dispozițiile prezentului regulament, inclusiv prin stabilirea unor sancțiuni efective, proporționale și cu efect de descurajare în cazul încălcării acestora, și pentru a respecta principiul *ne bis in idem*. În scopul de a consolida și armoniza sancțiunile administrative pentru încălcarea prezentului regulament, ar trebui să fie definite limitele superioare pentru stabilirea amenzilor administrative pentru anumite încălcări specifice. Atunci când evaluează cuantumul amenzilor, statele membre ar trebui, în fiecare caz în parte, să țină seama de toate circumstanțele relevante ale situației specifice, acordând atenția cuvenită, în special, naturii, gravității și duratei încălcării și consecințelor acesteia, precum și dimensiunii furnizorului, în special în cazul în care furnizorul este un IMM, inclusiv o întreprindere nou-înființată. Autoritatea Europeană pentru Protecția Datelor ar trebui să aibă competența de a impune amenzi instituțiilor, agențiilor și organelor Uniunii care intră în domeniul de aplicare al prezentului regulament.
- (169) Respectarea obligațiilor impuse furnizorilor de modele de IA de uz general în temeiul prezentului regulament ar trebui să fie asigurată, printre altele, prin amenzi. În acest scop, ar trebui să fie stabilite, de asemenea, niveluri adecvate ale amenzilor pentru încălcarea obligațiilor respective, inclusiv pentru nerespectarea măsurilor impuse de Comisie în conformitate cu prezentul regulament, sub rezerva unor termene de prescripție adecvate, în conformitate cu principiul proporționalității. Toate deciziile luate de Comisie în temeiul prezentului regulament fac obiectul controlului jurisdicțional al Curții de Justiție a Uniunii Europene în conformitate cu TFUE, incluzând competența nelimitată a Curții de Justiție cu privire la sancțiuni în temeiul articolului 261 din TFUE.

- (170) Dreptul Uniunii și dreptul intern prevăd deja căi de atac efective pentru persoanele fizice și juridice ale căror drepturi și libertăți sunt afectate în mod negativ de utilizarea sistemelor de IA. Fără a aduce atingere căilor de atac respective, orice persoană fizică sau juridică care are motive să considere că a avut loc o încălcare a prezentului regulament ar trebui să aibă dreptul de a depune o plângere la autoritatea relevantă de supraveghere a pieței.
- (171) Persoanele afectate ar trebui să aibă dreptul de a obține o explicație atunci când decizia implementatorului este bazată în principal pe rezultatele anumitor sisteme de IA cu grad ridicat de risc care intră în domeniul de aplicare al prezentului regulament și în cazul în care decizia respectivă produce efecte juridice sau afectează în mod similar în mod semnificativ persoanele respective într-o manieră pe care acestea o consideră ca având un impact negativ asupra sănătății, siguranței sau drepturilor fundamentale ale acestora. Explicația respectivă ar trebui să fie clară și semnificativă și să ofere un temei pentru exercitarea drepturilor de către persoanele afectate. Dreptul de a obține o explicație nu ar trebui să se aplice în cazul utilizării unor sisteme de IA care fac obiectul unor excepții sau restricții care decurg din dreptul Uniunii sau din dreptul intern și ar trebui să se aplice numai în măsura în care acest drept nu este deja prevăzut în dreptul Uniunii.
- (172) Persoanele care acționează în calitate de avertizori de integritate cu privire la încălcările prezentului regulament ar trebui să fie protejate în temeiul dreptului Uniunii. În ceea ce privește raportarea încălcărilor prezentului regulament și protecția persoanelor care raportează astfel de încălcări ar trebui, prin urmare, să se aplice Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului⁵⁴.

⁵⁴ Directiva (UE) 2019/1937 a Parlamentului European și a Consiliului din 23 octombrie 2019 privind protecția persoanelor care raportează încălcări ale dreptului Uniunii (JO L 305, 26.11.2019, p. 17).

(173) Pentru a se asigura posibilitatea de adaptare a cadrului de reglementare atunci când este necesar, competența de a adopta acte în conformitate cu articolul 290 din TFUE ar trebui să fie delegată Comisiei pentru a modifica condițiile în care un sistem de IA nu este considerat ca având un grad ridicat de risc, lista sistemelor de IA cu grad ridicat de risc, dispozițiile privind documentația tehnică, conținutul declarației de conformitate UE, dispozițiile privind procedurile de evaluare a conformității, dispozițiile de stabilire a sistemelor de IA cu grad ridicat de risc cărora ar trebui să li se aplice procedura de evaluare a conformității bazată pe evaluarea sistemului de management al calității și pe evaluarea documentației tehnice, pragul, valorile de referință și indicatorii din cadrul normelor pentru clasificarea modelelor de IA de uz general cu risc sistemic, inclusiv prin completarea valorilor de referință și indicatorilor respectivi, criteriile pentru desemnarea modelelor de IA de uz general cu risc sistemic, documentația tehnică pentru furnizorii de modele de IA de uz general și informațiile privind transparența pentru furnizorii de modele de IA de uz general. Este deosebit de important ca, în cursul lucrărilor sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți, și ca respectivele consultări să se desfășoare în conformitate cu principiile stabilite în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare⁵⁵. În special, pentru a asigura participarea egală la pregătirea actelor delegate, Parlamentul European și Consiliul primesc toate documentele în același timp cu experții din statele membre, iar experții acestor instituții au acces sistematic la reuniunile grupurilor de experți ale Comisiei însărcinate cu pregătirea actelor delegate.

⁵⁵ JO L 123, 12.5.2016, p. 1.

(174) Având în vedere evoluțiile tehnologice rapide și cunoștințele de specialitate tehnice necesare pentru aplicarea eficientă a prezentului regulament, Comisia ar trebui să evalueze și să revizuiască prezentul regulament până la ... [cinci ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani și să raporteze Parlamentului European și Consiliului în acest sens. În plus, ținând seama de implicațiile pentru domeniul de aplicare al prezentului regulament, Comisia ar trebui să efectueze o evaluare a necesității de a modifica, o dată pe an, lista sistemelor de IA cu grad ridicat de risc și lista practicilor interzise. În plus, până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia ar trebui să evalueze necesitatea de a modifica lista rubricilor de domeniu cu grad ridicat de risc din anexa la prezentul regulament, sistemele de IA care intră în domeniul de aplicare al obligațiilor de transparență, eficacitatea sistemului de supraveghere și de guvernanță și progresele înregistrate în ceea ce privește elaborarea de documente de standardizare privind dezvoltarea eficientă din punct de vedere energetic a modelelor de IA de uz general, inclusiv necesitatea unor măsuri sau acțiuni suplimentare și să raporteze Parlamentului European și Consiliului în acest sens. În cele din urmă, până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la trei ani, Comisia ar trebui să evalueze impactul și eficacitatea codurilor de conduită voluntare în ceea ce privește încurajarea aplicării cerințelor prevăzute pentru sistemele de IA cu grad ridicat de risc în cazul altor sisteme de IA decât cele cu grad ridicat de risc și, eventual, a altor cerințe suplimentare pentru sistemele de IA respective.

- (175) În vederea asigurării unor condiții uniforme pentru punerea în aplicare a prezentului regulament, ar trebui să fie conferite competențe de executare Comisiei. Respectivele competențe ar trebui să fie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului⁵⁶.
- (176) Întrucât obiectivul prezentului regulament, și anume de a îmbunătăți funcționarea pieței interne și de a promova adoptarea IA centrate pe factorul uman și fiabile, asigurând în același timp un nivel ridicat de protecție a sănătății, a siguranței și a drepturilor fundamentale consacrate în Cartă, inclusiv a democrației, a statului de drept și a mediului împotriva efectelor dăunătoare ale sistemelor de IA din Uniune, și sprijinind inovarea, nu poate fi realizat în mod satisfăcător de către statele membre și, având în vedere amploarea sau efectele acțiunii sale, poate fi realizat mai bine la nivelul Uniunii, aceasta din urmă poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum se prevede la articolul 5 din TUE. În conformitate cu principiul proporționalității, astfel cum este definit la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru realizarea obiectivului menționat.

⁵⁶ Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

- (177) Pentru a asigura securitatea juridică, a asigura o perioadă de adaptare adecvată pentru operatori și a evita perturbarea pieței, inclusiv prin asigurarea continuității utilizării sistemelor de IA, este oportun ca prezentul regulament să se aplice sistemelor de IA cu grad ridicat de risc care au fost introduse pe piață sau puse în funcțiune înainte de data generală de aplicare a acestuia, numai dacă, de la data respectivă, sistemele respective fac obiectul unor modificări semnificative în ceea ce privește proiectarea sau scopul lor preconizat. Este oportun să se clarifice că, în acest sens, conceptul de modificare semnificativă ar trebui să fie înțeles ca fiind echivalent în esență cu noțiunea de modificare substanțială, care este utilizată numai în ceea ce privește sistemele de IA cu grad ridicat de risc, în temeiul prezentului regulament. În mod excepțional și având în vedere răspunderea publică, operatorii de sisteme de IA care fac parte din sistemele informatice la scară largă instituite prin actele juridice care sunt enumerate într-o anexă la prezentul regulament și operatorii de sisteme de IA cu grad ridicat de risc care sunt destinate a fi utilizate de autoritățile publice ar trebui să ia măsurile necesare pentru a se conforma cerințelor prezentului regulament până la sfârșitul anului 2030 și, respectiv, până la ... [șase ani de la data intrării în vigoare a prezentului regulament].
- (178) Furnizorii de sisteme de IA cu grad ridicat de risc sunt încurajați să înceapă să se conformeze, în mod voluntar, obligațiilor relevante aferente prezentului regulament încă din perioada de tranziție.

(179) Prezentul regulament ar trebui să se aplice de la ... [doi ani de la data intrării în vigoare a prezentului regulament]. Cu toate acestea, ținând seama de riscul inacceptabil asociat utilizării IA în anumite moduri, interdicțiile și dispozițiile cu caracter general din prezentul regulament ar trebui să se aplice deja de la ... [șase luni de la data intrării în vigoare a prezentului regulament]. Deși efectul deplin al interdicțiilor respective este corelat cu instituirea guvernantei și cu aplicarea prezentului regulament, aplicarea anticipată a interdicțiilor este importantă pentru a se ține seama de riscurile inacceptabile și pentru a produce efecte asupra altor proceduri, cum ar fi în dreptul civil. În plus, infrastructura legată de guvernanta și de sistemul de evaluare a conformității ar trebui să fie operațională înainte de ... [doi ani de la data intrării în vigoare a prezentului regulament]; prin urmare, dispozițiile privind organismele notificate și structura de guvernanta ar trebui să se aplice de la ... [12 luni de la data intrării în vigoare a prezentului regulament]. Având în vedere ritmul rapid al progreselor tehnologice și al adoptării modelelor de IA de uz general, ar trebui ca obligațiile furnizorilor de modele de IA de uz general să se aplice de la ... [12 luni de la data intrării în vigoare a prezentului regulament]. Codurile de bune practici ar trebui să fie gata până la ... [nouă luni de la data intrării în vigoare a prezentului regulament], pentru a permite furnizorilor să demonstreze conformitatea în timp util. Oficiul pentru IA ar trebui să se asigure că normele și procedurile de clasificare sunt actualizate în funcție de evoluțiile tehnologice. În plus, statele membre ar trebui să stabilească și să notifice Comisiei normele privind sancțiunile, inclusiv amenzile administrative, și să se asigure că acestea sunt puse în aplicare în mod corespunzător și efectiv până la data aplicării prezentului regulament. Prin urmare, dispozițiile privind sancțiunile ar trebui să se aplice de la ... [12 luni de la data intrării în vigoare a prezentului regulament].

(180) Autoritatea Europeană pentru Protecția Datelor și Comitetul european pentru protecția datelor au fost consultate în conformitate cu articolul 42 alineatele (1) și (2) din Regulamentul (UE) 2018/1725 și au emis avizul lor comun la 18 iunie 2021,

ADOPTĂ PREZENTUL REGULAMENT:

Capitolul I

Dispoziții generale

Articolul 1

Obiectul

- (1) Scopul prezentului regulament este de a îmbunătăți funcționarea pieței interne, de a promova adoptarea inteligenței artificiale (IA) centrate pe factorul uman și fiabile, asigurând în același timp un nivel ridicat de protecție a sănătății, a siguranței și a drepturilor fundamentale consacrate în Cartă, inclusiv a democrației, a statului de drept și a mediului împotriva efectelor dăunătoare ale sistemelor de IA din Uniune, și sprijinind inovarea.
- (2) Prezentul regulament stabilește:
 - (a) norme armonizate pentru introducerea pe piață, punerea în funcțiune și utilizarea sistemelor de IA în Uniune;
 - (b) interdicții privind anumite practici în domeniul IA;
 - (c) cerințe specifice pentru sistemele de IA cu grad ridicat de risc și obligații pentru operatorii unor astfel de sisteme;
 - (d) norme armonizate de transparență pentru anumite sisteme de IA;
 - (e) norme armonizate privind introducerea pe piață a modelelor de IA de uz general;

- (f) norme privind monitorizarea pieței, supravegherea pieței, guvernanta și aplicarea prezentului regulament;
- (g) măsuri de susținere a inovării, cu un accent deosebit pe IMM-uri, inclusiv pe întreprinderile nou-înființate.

Articolul 2
Domeniul de aplicare

- (1) Prezentul regulament se aplică pentru:
 - (a) furnizorii care introduc pe piață sau pun în funcțiune sisteme de IA sau introduc pe piață modele de IA de uz general în Uniune, indiferent dacă furnizorii respectivi sunt stabiliți sau se află în Uniune sau într-o țară terță;
 - (b) implementatorii de sisteme de IA care își au sediul sau se află pe teritoriul Uniunii;
 - (c) furnizorii și implementatorii de sisteme de IA care își au sediul sau se află într-o țară terță, în cazul în care rezultatele produse de sistemele de IA sunt utilizate în Uniune;
 - (d) importatorii și distribuitorii de sisteme de IA;
 - (e) fabricanții de produse care introduc pe piață sau pun în funcțiune un sistem de IA împreună cu produsul lor și sub numele sau marca lor comercială;
 - (f) reprezentanții autorizați ai furnizorilor, care nu sunt stabiliți în Uniune;
 - (g) persoanele afectate care se află în Uniune.

- (2) În cazul sistemelor de IA clasificate ca sisteme de IA prezentând un grad ridicat de risc în conformitate cu articolul 6 alineatul (1), legate de produse care fac obiectul actelor legislative de armonizare ale Uniunii care figurează în anexa I secțiunea B, se aplică numai articolul 6 alineatul (1), articolele 102-109 și articolul 112. Articolul 57 se aplică numai în măsura în care cerințele pentru sistemele de IA cu grad ridicat de risc prevăzute în temeiul prezentului regulament au fost integrate în respectivele acte legislative de armonizare ale Uniunii.
- (3) Prezentul regulament nu se aplică domeniilor care nu intră în sfera de cuprindere a dreptului Uniunii și, în orice caz, nu afectează competențele statelor membre în materie de securitate națională, indiferent de tipul de entitate însărcinată de statele membre să îndeplinească sarcinile legate de competențele respective.

Prezentul regulament nu se aplică sistemelor de IA în cazul și în măsura în care sunt introduse pe piață, puse în funcțiune sau utilizate cu sau fără modificări exclusiv în scopuri militare, de apărare sau de securitate națională, indiferent de tipul de entitate care desfășoară activitățile respective.

Prezentul regulament nu se aplică sistemelor de IA care nu sunt introduse pe piață sau puse în funcțiune în Uniune, în cazul în care rezultatul este utilizat în Uniune exclusiv în scopuri militare, de apărare sau de securitate națională, indiferent de tipul de entitate care desfășoară activitățile respective.

- (4) Prezentul regulament nu se aplică autorităților publice dintr-o țară terță și nici organizațiilor internaționale care intră în sfera de cuprindere a prezentului regulament în temeiul alineatului (1), în cazul în care respectivele autorități sau organizații utilizează sisteme de IA în cadrul cooperării sau acordurilor internaționale pentru aplicarea legii și pentru cooperarea judiciară cu Uniunea sau cu unul sau mai multe state membre, cu condiția ca o astfel de țară terță sau organizație internațională să ofere garanții adecvate în ceea ce privește protecția drepturilor și libertăților fundamentale ale persoanelor.
- (5) Prezentul regulament nu aduce atingere aplicării dispozițiilor privind răspunderea furnizorilor de servicii intermediare cuprinse în capitolul II din Regulamentul (UE) 2022/2065.
- (6) Prezentul regulament nu se aplică sistemelor de IA sau modelelor de IA, inclusiv rezultatelor acestora, dezvoltate și puse în funcțiune special și exclusiv pentru cercetare și dezvoltare științifică.
- (7) Dreptul Uniunii privind protecția datelor cu caracter personal, a vieții private și a confidențialității comunicațiilor se aplică datelor cu caracter personal prelucrate în legătură cu drepturile și obligațiile prevăzute în prezentul regulament. Prezentul regulament nu afectează Regulamentul (UE) 2016/679 sau (UE) 2018/1725 ori Directiva 2002/58/CE sau (UE) 2016/680, fără a aduce atingere articolului 10 alineatul (5) și articolului 59 din prezentul regulament.
- (8) Prezentul regulament nu se aplică niciunei activități de cercetare, testare sau dezvoltare privind sisteme de IA sau modele de IA, înainte ca acestea să fie introduse pe piață sau puse în funcțiune. Astfel de activități se desfășoară în conformitate cu dreptul aplicabil al Uniunii. Testarea în condiții reale nu face obiectul excluderii menționate.

- (9) Prezentul regulament nu aduce atingere normelor prevăzute de alte acte juridice ale Uniunii referitoare la protecția consumatorilor și la siguranța produselor.
- (10) Prezentul regulament nu se aplică obligațiilor implementatorilor persoane fizice care utilizează sisteme de IA în cursul unei activități strict personale, fără caracter profesional.
- (11) Prezentul regulament nu împiedică Uniunea sau statele membre să mențină sau să introducă acte cu putere de lege și acte administrative care sunt mai favorabile lucrătorilor privind protejarea drepturilor acestora în ceea ce privește utilizarea sistemelor de IA de către angajatori sau să încurajeze ori să permită aplicarea unor contracte colective de muncă care sunt mai favorabile lucrătorilor.
- (12) Prezentul regulament nu se aplică sistemelor de IA lansate sub licențe libere și cu sursă deschisă, cu excepția cazului în care acestea sunt introduse pe piață sau puse în funcțiune ca sisteme de IA cu grad ridicat de risc sau ca sisteme de IA care intră sub incidența articolului 5 sau a articolului 50.

Articolul 3

Definiții

În sensul prezentului regulament, se aplică următoarele definiții:

1. „sistem de IA” înseamnă un sistem bazat pe o mașină care este conceput să funcționeze cu diferite niveluri de autonomie și care poate prezenta adaptabilitate după implementare, și care, urmărind obiective explicite sau implicite, deduce, din datele de intrare pe care le primește, modul de generare a unor rezultate precum previziuni, conținut, recomandări sau decizii care pot influența mediile fizice sau virtuale;

2. „risc” înseamnă combinația dintre probabilitatea producerii unui prejudiciu și gravitatea acestuia;
3. „furnizor” înseamnă o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care dezvoltă un sistem de IA sau un model de IA de uz general sau care comandă dezvoltarea unui sistem de IA sau a unui model de IA de uz general și îl introduce pe piață sau pune în funcțiune sistemul de IA sub propriul nume sau propria marcă comercială, contra cost sau gratuit;
4. „implementator” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau alt organism care utilizează un sistem de IA aflat sub autoritatea sa, cu excepția cazului în care sistemul de IA este utilizat în cursul unei activități personale, fără caracter profesional;
5. „reprezentant autorizat” înseamnă o persoană fizică sau juridică aflată sau stabilită în Uniune care a primit și a acceptat un mandat scris din partea unui furnizor al unui sistem de IA sau al unui model de IA de uz general pentru a exercita și, respectiv, a îndeplini, în numele său, obligațiile și procedurile stabilite prin prezentul regulament;
6. „importator” înseamnă o persoană fizică sau juridică aflată sau stabilită în Uniune care introduce pe piață un sistem de IA care poartă numele sau marca unei persoane fizice sau juridice stabilite într-o țară terță;
7. „distribuitor” înseamnă o persoană fizică sau juridică din lanțul de aprovizionare, alta decât furnizorul sau importatorul, care pune la dispoziție un sistem de IA pe piața Uniunii;
8. „operator” înseamnă furnizor, fabricant de produse, implementator, reprezentant autorizat, importator sau distribuitor;

9. „introducere pe piață” înseamnă prima punere la dispoziție a unui sistem de IA sau a unui model de IA de uz general pe piața Uniunii;
10. „punere la dispoziție pe piață” înseamnă furnizarea unui sistem de IA sau a unui model de IA de uz general pentru distribuție sau uz pe piața Uniunii în cursul unei activități comerciale, contra cost sau gratuit;
11. „punere în funcțiune” înseamnă furnizarea unui sistem de IA pentru prima utilizare direct implementatorului sau pentru uz propriu în Uniune, în scopul său preconizat;
12. „scop preconizat” înseamnă utilizarea preconizată de către furnizor a unui sistem de IA, inclusiv contextul specific și condițiile de utilizare, astfel cum se specifică în informațiile oferite de furnizor în instrucțiunile de utilizare, în materialele promoționale sau de vânzare și în declarații, precum și în documentația tehnică;
13. „utilizare necorespunzătoare previzibilă în mod rezonabil” înseamnă utilizarea unui sistem de IA într-un mod care nu este în conformitate cu scopul său preconizat, dar care poate rezulta din comportamentul uman sau din interacțiunea previzibilă în mod rezonabil cu alte sisteme, inclusiv cu alte sisteme de IA;
14. „componentă de siguranță” înseamnă o componentă a unui produs sau a unui sistem de IA care îndeplinește o funcție de siguranță pentru produsul sau sistemul de IA respectiv sau a cărei defectare sau funcționare defectuoasă pune în pericol sănătatea și siguranța persoanelor sau a bunurilor;
15. „instrucțiuni de utilizare” înseamnă informațiile oferite de furnizor pentru a informa implementatorul, în special cu privire la scopul preconizat și utilizarea corespunzătoare a unui sistem de IA;

16. „rechemare a unui sistem de IA” înseamnă orice măsură care are drept scop returnarea către furnizor, scoaterea din funcțiune sau dezactivarea utilizării unui sistem de IA deja pus la dispoziția implementatorilor;
17. „retragere a unui sistem de IA” înseamnă orice măsură care are drept scop împiedicarea punerii la dispoziție pe piață a unui sistem de IA din lanțul de aprovizionare;
18. „performanță a unui sistem de IA” înseamnă capacitatea unui sistem de IA de a-și îndeplini scopul preconizat;
19. „autoritate de notificare” înseamnă autoritatea națională responsabilă cu instituirea și îndeplinirea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora;
20. „evaluare a conformității” înseamnă procesul prin care se demonstrează dacă au fost îndeplinite sau nu cerințele prevăzute în capitolul III secțiunea 2 referitoare la un sistem de IA cu grad ridicat de risc;
21. „organism de evaluare a conformității” înseamnă un organism care efectuează activități de evaluare a conformității ca parte terță, incluzând testarea, certificarea și inspecția;
22. „organism notificat” înseamnă un organism de evaluare a conformității notificat în conformitate cu prezentul regulament și cu alte acte legislative relevante de armonizare ale Uniunii;
23. „modificare substanțială” înseamnă o modificare a unui sistem de IA după introducerea sa pe piață sau punerea sa în funcțiune, care nu este prevăzută sau planificată în evaluarea inițială a conformității realizată de furnizor și în urma căreia este afectată conformitatea sistemului de IA cu cerințele prevăzute în capitolul III secțiunea 2 sau care conduce la o modificare a scopului preconizat pentru care a fost evaluat sistemul de IA;

24. „marcaj CE” înseamnă un marcaj prin care un furnizor indică faptul că un sistem de IA este în conformitate cu cerințele prevăzute în capitolul III secțiunea 2 și în alte acte legislative de armonizare aplicabile ale Uniunii care prevăd aplicarea acestui marcaj;
25. „sistem de monitorizare ulterioară introducerii pe piață” înseamnă toate activitățile desfășurate de furnizorii de sisteme de IA pentru a colecta și a revizui experiența dobândită în urma utilizării sistemelor de IA pe care le introduc pe piață sau le pun în funcțiune, în scopul identificării oricărei nevoi de a aplica imediat orice măsură corectivă sau preventivă necesară;
26. „autoritate de supraveghere a pieței” înseamnă autoritatea națională care desfășoară activități și ia măsuri în temeiul Regulamentului (UE) 2019/1020;
27. „standard armonizat” înseamnă un standard armonizat, în sensul definiției de la articolul 2 punctul 1 litera (c) din Regulamentul (UE) nr. 1025/2012;
28. „specificație comună” înseamnă un set de specificații tehnice, astfel cum sunt definite la articolul 2 punctul 4 din Regulamentul (UE) nr. 1025/2012, care oferă mijloacele de a respecta anumite cerințe stabilite în temeiul prezentului regulament;
29. „date de antrenament” înseamnă datele utilizate pentru antrenarea unui sistem de IA prin adaptarea parametrilor săi care pot fi învățați;
30. „date de validare” înseamnă datele utilizate pentru a furniza o evaluare a sistemului de IA antrenat și pentru a-i ajusta parametrii care nu pot fi învățați și procesul său de învățare, printre altele, pentru a preveni subadaptarea sau supraadaptarea;

31. „set de date de validare” înseamnă un set de date separat sau o parte a setului de date de antrenament, sub forma unei divizări fixe sau variabile;
32. „date de testare” înseamnă datele utilizate pentru a furniza o evaluare independentă a sistemului de IA, în scopul de a confirma performanța preconizată a sistemului respectiv înainte de introducerea sa pe piață sau de punerea sa în funcțiune;
33. „date de intrare” înseamnă datele furnizate unui sistem de IA sau dobândite direct de acesta, pe baza cărora sistemul produce un rezultat;
34. „date biometrice” înseamnă datele cu caracter personal rezultate dintr-o prelucrare tehnică specifică, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice;
35. „identificare biometrică” înseamnă recunoașterea automată a caracteristicilor fizice, fiziologice, comportamentale sau psihologice ale omului în scopul stabilirii identității unei persoane fizice prin compararea datelor biometrice ale persoanei respective cu datele biometrice ale persoanelor stocate într-o bază de date;
36. „verificare biometrică” înseamnă verificarea automată, pe baza unei comparații între două seturi de date, inclusiv autentificarea, a identității persoanelor fizice prin compararea datelor biometrice ale acestora cu datele biometrice furnizate anterior;
37. „categorii speciale de date cu caracter personal” înseamnă categoriile de date cu caracter personal menționate la articolul 9 alineatul (1) din Regulamentul (UE) 2016/679, la articolul 10 din Directiva (UE) 2016/680 și la articolul 10 alineatul (1) din Regulamentul (UE) 2018/1725;

38. „date operaționale sensibile” înseamnă date operaționale legate de activități de prevenire, depistare, investigare sau urmărire penală a infracțiunilor a căror divulgare ar putea pune în pericol integritatea unor proceduri penale;
39. „sistem de recunoaștere a emoțiilor” înseamnă un sistem de IA al cărui scop este de a identifica sau a deduce emoțiile sau intențiile persoanelor fizice pe baza datelor lor biometrice;
40. „sistem de clasificare biometrică” înseamnă un sistem de IA al cărui scop este de a încadra persoanele fizice în categorii specifice pe baza datelor lor biometrice, cu excepția cazului în care acesta este auxiliar unui alt serviciu comercial și strict necesar din motive tehnice obiective;
41. „sistem de identificare biometrică la distanță” înseamnă un sistem de IA al cărui scop este de a identifica persoanele fizice, fără implicarea activă a acestora, de obicei la distanță, prin compararea datelor biometrice ale unei persoane cu datele biometrice conținute într-o bază de date de referință;
42. „sistem de identificare biometrică la distanță în timp real” înseamnă un sistem de identificare biometrică la distanță în care atât capturarea datelor biometrice, cât și compararea și identificarea au loc fără întârzieri semnificative, incluzând nu numai identificarea instantanee, ci și întârzieri scurte limitate pentru a se evita eludarea;
43. „sistem de identificare biometrică la distanță ulterioară” înseamnă un alt sistem de identificare biometrică la distanță decât sistemul de identificare biometrică la distanță în timp real;

44. „spațiu accesibil publicului” înseamnă orice loc fizic aflat în proprietate publică sau privată, accesibil unui număr nedeterminat de persoane fizice, indiferent dacă se pot aplica anumite condiții de acces și indiferent de potențiale restricții de capacitate;
45. „autoritate de aplicare a legii” înseamnă:
- (a) orice autoritate publică competentă în materie de prevenire, investigare, depistare sau urmărire penală a infracțiunilor sau de executare a sancțiunilor penale, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau
 - (b) orice alt organism sau entitate împuternicit(ă) de dreptul statului membru să exercite autoritate publică și competențe publice în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora;
46. „aplicarea legii” înseamnă activitățile desfășurate de autoritățile de aplicare a legii sau în numele acestora pentru prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau pentru executarea sancțiunilor penale, inclusiv pentru protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
47. „Oficiul pentru IA” înseamnă funcția Comisiei de a contribui la punerea în aplicare, monitorizarea și supravegherea sistemelor de IA și a modelelor de IA de uz general și la guvernanta IA, prevăzută în Decizia din 24 ianuarie 2024 a Comisiei; trimiterile din prezentul regulament la Oficiul pentru IA se interpretează ca trimiteri la Comisie;

48. „autoritate națională competentă” înseamnă o autoritate de notificare sau o autoritate de supraveghere a pieței; în ceea ce privește sistemele de IA puse în funcțiune sau utilizate de instituțiile, agențiile, oficiile și organele Uniunii, mențiunile referitoare la autoritățile naționale competente sau la autoritățile de supraveghere a pieței din prezentul regulament se interpretează ca mențiuni referitoare la Autoritatea Europeană pentru Protecția Datelor;
49. „incident grav” înseamnă un incident sau funcționarea necorespunzătoare a unui sistem de IA care, direct sau indirect, conduce la oricare dintre următoarele:
- (a) decesul unei persoane sau vătămarea gravă a sănătății unei persoane;
 - (b) o perturbare gravă și ireversibilă a gestionării sau a funcționării infrastructurii critice;
 - (c) încălcarea obligațiilor care decurg din dreptul Uniunii menit să protejeze drepturile fundamentale;
 - (d) daune grave aduse bunurilor sau mediului;
50. „date cu caracter personal” înseamnă datele cu caracter personal astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;
51. „date fără caracter personal” înseamnă date, altele decât datele cu caracter personal definite la articolul 4 punctul 1 din Regulamentul (UE) 2016/679;
52. „creare de profiluri” înseamnă creare de profiluri în sensul definiției de la articolul 4 punctul 4 din Regulamentul (UE) 2016/679;

53. „plan de testare în condiții reale” înseamnă un document care descrie obiectivele, metodologia, domeniul de aplicare geografic, demografic și temporal, monitorizarea, organizarea și efectuarea testelor în condiții reale;
54. „plan privind spațiul de testare” înseamnă un document convenit între furnizorul participant și autoritatea competentă care descrie obiectivele, condițiile, calendarul, metodologia și cerințele pentru activitățile desfășurate în spațiul de testare;
55. „spațiu de testare în materie de reglementare în domeniul IA” înseamnă un cadru controlat instituit de o autoritate competentă care oferă furnizorilor sau potențialilor furnizori de sisteme de IA posibilitatea de a dezvolta, de a antrena, de a valida și de a testa, după caz în condiții reale, un sistem de IA inovator, pe baza unui plan privind spațiul de testare, pentru o perioadă limitată de timp, sub supraveghere reglementară;
56. „alfabetizare în domeniul IA” înseamnă competențele, cunoștințele și înțelegerea care le permit furnizorilor, implementatorilor și persoanelor afectate, ținând seama de drepturile și obligațiile lor respective în contextul prezentului regulament, să implementeze sistemele de IA în cunoștință de cauză și să conștientizeze oportunitățile și riscurile pe care le implică IA, precum și prejudiciile pe care le pot aduce;
57. „testare în condiții reale” înseamnă testarea temporară a unui sistem de IA în scopul său preconizat, în condiții reale, în afara unui laborator sau a unui mediu simulat în alt mod, în vederea colectării de date fiabile și solide și a evaluării și verificării conformității sistemului de IA cu cerințele prezentului regulament și nu se consideră introducere pe piață sau punere în funcțiune a sistemului de IA în sensul prezentului regulament, dacă sunt îndeplinite toate condițiile prevăzute la articolul 57 sau 60;

58. „subiect” în scopul testării în condiții reale înseamnă o persoană fizică care participă la testarea în condiții reale;
59. „consimțământ în cunoștință de cauză” înseamnă exprimarea liberă, specifică, neechivocă și voluntară de către un subiect a dorinței sale de a participa la o anumită testare în condiții reale, după ce a fost informat cu privire la toate aspectele testării care sunt relevante pentru decizia sa de a participa;
60. „deepfake” înseamnă o imagine ori un conținut audio sau video generat sau manipulat de IA care prezintă o asemănare cu persoane, obiecte, locuri sau alte entități ori evenimente existente și care ar crea unei persoane impresia falsă că este autentic sau adevărat;
61. „încălcare pe scară largă” înseamnă orice acțiuni sau omisiuni contrare dreptului Uniunii care protejează interesele persoanelor fizice și care:
- (a) au adus sau ar putea aduce prejudicii intereselor colective ale persoanelor care își au reședința în cel puțin două state membre diferite de statul membru în care:
 - (i) au fost inițiate sau au avut loc acțiunile sau omisiunile în cauză;
 - (ii) se află sau este stabilit furnizorul în cauză sau, după caz, reprezentantul său autorizat; sau
 - (iii) este stabilit implementatorul, atunci când încălcarea este comisă de implementator;

- (b) au adus, aduc sau sunt susceptibile să aducă prejudicii intereselor colective ale persoanelor și au caracteristici comune, cum ar fi aceeași practică ilegală, încălcarea aceluiași interes, care survin în același timp, fiind comise de același operator, în cel puțin trei state membre;
62. „infrastructură critică” înseamnă infrastructură critică în sensul definiției de la articolul 2 punctul 4 din Directiva (UE) 2022/2557;
63. „model de IA de uz general” înseamnă un model de IA, inclusiv în cazul în care un astfel de model de IA este antrenat cu un volum mare de date care utilizează autosupravegherea la scară largă, care prezintă o generalitate semnificativă și este capabil să îndeplinească în mod competent o gamă largă de sarcini distincte, indiferent de modul în care este introdus pe piață și care poate fi integrat într-o varietate de sisteme sau aplicații din aval, cu excepția modelelor de IA care sunt utilizate pentru activități de cercetare, dezvoltare sau creare de prototipuri înainte de introducerea pe piață;
64. „capabilități cu impact ridicat” înseamnă capabilități care corespund capabilităților înregistrate în cele mai avansate modele de IA de uz general sau depășesc capabilitățile respective;
65. „risc sistemic” înseamnă un risc specific capabilităților cu impact ridicat ale modelelor de IA de uz general, având un impact semnificativ asupra pieței Uniunii ca urmare a amplorii acestora sau a efectelor negative reale sau previzibile în mod rezonabil asupra sănătății publice, siguranței, securității publice, drepturilor fundamentale sau asupra societății în ansamblu, care poate fi propagat la scară largă de-a lungul lanțului valoric;

66. „sistem de IA de uz general” înseamnă un sistem de IA care se bazează pe un model de IA de uz general și care are capacitatea de a deservi o varietate de scopuri, atât pentru utilizare directă, cât și pentru integrarea în alte sisteme de IA;
67. „operație în virgulă mobilă” înseamnă orice operație matematică sau atribuire care implică numere în virgulă mobilă, care sunt o subcategorie a numerelor reale și sunt reprezentate de regulă în informatică printr-un număr întreg cu precizie fixă multiplicat cu o bază fixă având un exponent număr întreg;
68. „furnizor din aval” înseamnă un furnizor al unui sistem de IA, inclusiv al unui sistem de IA de uz general, care integrează un model de IA, indiferent dacă modelul de IA este furnizat de furnizorul însuși și integrat vertical sau dacă acesta este furnizat de o altă entitate pe baza unor relații contractuale.

Articolul 4

Alfabetizarea în domeniul IA

Furnizorii și implementatorii de sisteme de IA iau măsuri pentru a asigura, în cea mai mare măsură posibilă, un nivel suficient de alfabetizare în domeniul IA a personalului lor și a altor persoane care se ocupă cu operarea și utilizarea sistemelor de IA în numele lor, ținând seama de cunoștințele tehnice, experiența, educația și formarea lor și de contextul în care urmează să fie folosite sistemele de IA și luând în considerare persoanele sau grupurile de persoane în legătură cu care urmează să fie folosite sistemele de IA.

Capitolul II

Practici interzise în domeniul IA

Articolul 5

Practici interzise în domeniul IA

- (1) Sunt interzise următoarele practici în domeniul IA:
- (a) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care utilizează tehnici subliminale ce nu pot fi percepute în mod conștient de o persoană sau tehnici intenționat manipulative sau înșelătoare, cu scopul sau efectul de a denatura în mod semnificativ comportamentul unei persoane sau al unui grup de persoane prin împiedicarea apreciabilă a capacității acestora de a lua o decizie în cunoștință de cauză, determinându-le astfel să ia o decizie pe care altfel nu ar fi luat-o, într-un mod care aduce sau este susceptibil în mod rezonabil să aducă prejudicii semnificative persoanei respective, unei alte persoane sau unui grup de persoane;
 - (b) introducerea pe piață, punerea în funcțiune sau utilizarea unui sistem de IA care exploatează oricare dintre vulnerabilitățile unei persoane fizice sau ale unui anumit grup de persoane asociate vârstei, unei dizabilități sau unei situații sociale sau economice specifice, cu scopul sau efectul de a denatura în mod semnificativ comportamentul persoanei respective sau al unei persoane care aparține grupului respectiv într-un mod care aduce sau este susceptibil în mod rezonabil să aducă prejudicii semnificative persoanei respective sau unei alte persoane;

- (c) introducerea pe piață, punerea în funcțiune sau utilizarea unor sisteme de IA pentru evaluarea sau clasificarea persoanelor fizice sau a grupurilor de persoane pe o anumită perioadă de timp, pe baza comportamentului lor social sau a caracteristicilor personale sau de personalitate cunoscute, deduse sau preconizate, cu un punctaj social care conduce la una dintre următoarele situații sau la ambele:
 - (i) tratamentul prejudiciabil sau nefavorabil aplicat anumitor persoane fizice sau unor grupuri de persoane în contexte sociale care nu au legătură cu contextele în care datele au fost generate sau colectate inițial;
 - (ii) tratamentul prejudiciabil sau nefavorabil aplicat anumitor persoane fizice sau unor grupuri de persoane, care este nejustificat sau disproporționat în raport cu comportamentul social al acestora sau cu gravitatea acestuia;
- (d) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unui sistem de IA pentru efectuarea de evaluări ale riscurilor persoanelor fizice cu scopul de a evalua sau de a prevedea riscul ca o persoană fizică să comită o infracțiune, exclusiv pe baza creării profilului unei persoane fizice sau pe baza evaluării trăsăturilor și caracteristicilor sale de personalitate; această interdicție nu se aplică sistemelor de IA utilizate pentru a sprijini evaluarea umană a implicării unei persoane într-o activitate infracțională, care se bazează deja pe fapte obiective și verificabile legate direct de o activitate infracțională;
- (e) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unor sisteme de IA care creează sau extind bazele de date de recunoaștere facială prin extragerea fără scop precis a imaginilor faciale de pe internet sau de pe înregistrările TVCI;

- (f) introducerea pe piață, punerea în funcțiune în acest scop specific sau utilizarea unor sisteme de IA pentru a deduce emoțiile unei persoane fizice în sfera locului de muncă și a instituțiilor de învățământ, cu excepția cazurilor în care utilizarea sistemului de IA este destinată a fi instituită sau introdusă pe piață din motive medicale sau de siguranță;
- (g) introducerea pe piață sau punerea în funcțiune în acest scop specific sau utilizarea de sisteme de clasificare biometrică care clasifică în mod individual persoanele fizice pe baza datelor lor biometrice pentru a deduce sau a intui rasa, opiniile politice, apartenența la un sindicat, convingerile religioase sau filozofice, viața sexuală sau orientarea sexuală ale persoanelor respective; această interdicție nu se referă la etichetarea sau filtrarea seturilor de date biometrice obținute în mod legal, cum ar fi imaginile, pe baza datelor biometrice sau la clasificarea datelor biometrice în domeniul aplicării legii;
- (h) utilizarea sistemelor de identificare biometrică la distanță în timp real în spații accesibile publicului în scopul aplicării legii, cu excepția cazului și în măsura în care o astfel de utilizare este strict necesară pentru unul dintre următoarele obiective:
 - (i) căutarea în mod specific a anumitor victime ale răpirii, traficului de persoane sau exploatarei sexuale a persoanelor, precum și căutarea persoanelor dispărute;
 - (ii) prevenirea unei amenințări specifice, substanțiale și iminente care vizează viața sau siguranța fizică a persoanelor fizice sau a unei amenințări reale și prezente sau reale și previzibile de atac terorist;

- (iii) localizarea sau identificarea unei persoane suspectate de săvârșirea unei infracțiuni, în scopul desfășurării unei investigații penale sau al urmăririi penale sau al executării unor sancțiuni penale pentru infracțiuni, menționate în anexa II și pasibile, în statul membru în cauză, de o pedeapsă privativă de libertate sau o măsură de siguranță privativă de libertate pentru o perioadă maximă de cel puțin patru ani;

Litera (h) de la primul paragraf nu aduce atingere articolului 9 din Regulamentul (UE) 2016/679 privind prelucrarea datelor biometrice în alte scopuri decât aplicarea legii.

- (2) Sistemele de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii pentru oricare dintre obiectivele menționate la alineatul (1) primul paragraf litera (h) se utilizează în scopurile prevăzute la alineatul (1) litera (h) numai pentru a confirma identitatea persoanei vizate în mod specific, ținându-se seama de următoarele elemente:
 - (a) natura situației care determină posibila utilizare, în special gravitatea, probabilitatea și amploarea prejudiciului care ar fi cauzat dacă sistemul nu ar fi utilizat;
 - (b) consecințele utilizării sistemului asupra drepturilor și libertăților tuturor persoanelor vizate, în special gravitatea, probabilitatea și amploarea acestor consecințe.

În plus, utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii pentru oricare dintre obiectivele menționate la alineatul (1) primul paragraf litera (h) de la prezentul articol respectă garanțiile și condițiile necesare și proporționale în ceea ce privește utilizarea în conformitate cu dreptul intern care autorizează utilizarea sistemelor respective, în special în ceea ce privește limitările temporale, geografice și legate de persoane. Utilizarea sistemului de identificare biometrică la distanță în timp real în spațiile accesibile publicului este autorizată numai dacă autoritatea de aplicare a legii a finalizat o evaluare a impactului asupra drepturilor fundamentale, astfel cum se prevede la articolul 27, și a înregistrat sistemul în baza de date a UE, în conformitate cu articolul 49. Cu toate acestea, în cazuri de urgență justificate în mod corespunzător, utilizarea sistemelor respective poate fi inițiată fără înregistrarea în baza de date a UE, cu condiția ca înregistrarea respectivă să fie finalizată fără întârzieri nejustificate.

- (3) În sensul alineatului (1) primul paragraf litera (h) și al alineatului (2), fiecare utilizare în scopul aplicării legii a unui sistem de identificare biometrică la distanță în timp real în spațiile accesibile publicului face obiectul unei autorizații prealabile acordate de o autoritate judiciară sau de o autoritate administrativă independentă a cărei decizie are efect obligatoriu din statul membru în care urmează să aibă loc utilizarea; autorizația respectivă este emisă pe baza unei cereri motivate și în conformitate cu normele detaliate de drept intern menționate la alineatul (5). Cu toate acestea, într-o situație de urgență justificată în mod corespunzător, utilizarea sistemului poate începe fără autorizație, cu condiția ca autorizația respectivă să fie solicitată fără întârzieri nejustificate, cel târziu în termen de 24 de ore. În cazul în care o astfel de autorizație este refuzată, utilizarea sistemului este oprită cu efect imediat și toate datele, precum și rezultatele și produsele obținute în cadrul utilizării respective sunt înlăturate și șterse imediat.

Autoritatea judiciară competentă sau o autoritate administrativă independentă a cărei decizie are efect obligatoriu acordă autorizația numai dacă este convinsă, pe baza unor dovezi obiective sau a unor indicii clare care i-au fost prezentate, că utilizarea sistemului de identificare biometrică la distanță în timp real în cauză este necesară și proporțională pentru realizarea unuia dintre obiectivele menționate la alineatul (1) primul paragraf litera (h), astfel cum a fost identificat în cerere și, în special, rămâne limitată la ceea ce este strict necesar din punctul de vedere al perioadei de timp, precum și al sferei de aplicare geografică și personală. Atunci când ia o decizie cu privire la cerere, autoritatea respectivă ia în considerare elementele menționate la alineatul (2). Nicio decizie care produce un efect juridic negativ asupra unei persoane nu poate fi luată exclusiv pe baza unui rezultat al sistemului de identificare biometrică la distanță în timp real.

- (4) Fără a aduce atingere alineatului (3), fiecare utilizare a unui sistem de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii este notificată autorității relevante de supraveghere a pieței și autorității naționale pentru protecția datelor, în conformitate cu normele naționale menționate la alineatul (5). Notificarea conține cel puțin informațiile specificate la alineatul (6) și nu include date operaționale sensibile.

- (5) Un stat membru poate decide să prevadă posibilitatea de a autoriza, integral sau parțial, utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii, în limitele și condițiile enumerate la alineatul (1) primul paragraf litera (h) și la alineatele (2) și (3). Statul membru în cauză stabilește în dreptul său intern normele detaliate necesare pentru solicitarea, eliberarea și exercitarea, precum și pentru supravegherea autorizațiilor menționate la alineatul (3) și pentru raportarea cu privire la acestea. Normele respective specifică, de asemenea, pentru care dintre obiectivele enumerate la alineatul (1) primul paragraf litera (h), inclusiv pentru care dintre infracțiunile menționate la litera (h) punctul (iii) de la alineatul respectiv, pot fi autorizate autoritățile competente să utilizeze respectivele sisteme în scopul aplicării legii. Statele membre notifică normele respective Comisiei în termen de cel mult 30 de zile de la adoptarea acestora. Statele membre pot introduce, în conformitate cu dreptul Uniunii, legi mai restrictive privind utilizarea sistemelor de identificare biometrică la distanță.
- (6) Autoritățile naționale de supraveghere a pieței și autoritățile naționale de protecție a datelor din statele membre care au fost notificate cu privire la utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii în temeiul alineatului (4) prezintă Comisiei rapoarte anuale cu privire la utilizarea respectivă. În acest scop, Comisia furnizează statelor membre și autorităților naționale de supraveghere a pieței și de protecție a datelor un model, inclusiv informații privind numărul deciziilor luate de autoritățile judiciare competente sau de o autoritate administrativă independentă a cărei decizie are efect obligatoriu, în ceea ce privește cererile de autorizare în conformitate cu alineatul (3), precum și rezultatul cererilor respective.

- (7) Comisia publică rapoarte anuale privind utilizarea sistemelor de identificare biometrică la distanță în timp real în spațiile accesibile publicului în scopul aplicării legii, pe baza datelor agregate din statele membre din cadrul rapoartelor anuale menționate la alineatul (6). Rapoartele anuale respective nu includ date operaționale sensibile ale activităților conexe de aplicare a legii.
- (8) Prezentul articol nu afectează interdicțiile care se aplică în cazul în care o practică în materie de IA încalcă alte dispoziții din dreptul Uniunii.

Capitolul III

Sisteme de IA cu grad ridicat de risc

SECȚIUNEA 1

CLASIFICAREA SISTEMELOR DE IA CA PREZENTÂND UN RISC RIDICAT

Articolul 6

Norme de clasificare pentru sistemele de IA cu grad ridicat de risc

- (1) Indiferent dacă un sistem de IA este introdus pe piață sau pus în funcțiune independent de produsele menționate la literele (a) și (b), respectivul sistem de IA este considerat ca prezentând un grad ridicat de risc în cazul în care sunt îndeplinite cumulativ următoarele două condiții:
- (a) sistemul de IA este destinat a fi utilizat ca o componentă de siguranță a unui produs sau sistemul de IA este el însuși un produs care face obiectul legislației de armonizare a Uniunii care figurează în anexa I;

(b) produsul a cărui componentă de siguranță în temeiul literei (a) este sistemul de IA sau sistemul de IA în sine ca produs trebuie să fie supus unei evaluări a conformității de către o terță parte, în vederea introducerii pe piață sau a punerii în funcțiune a produsului respectiv în temeiul legislației de armonizare a Uniunii care figurează în anexa I.

(2) Sistemele de IA menționate în anexa III sunt considerate, pe lângă sistemele de IA cu grad ridicat de risc menționate la alineatul (1), ca prezentând un grad ridicat de risc.

(3) Prin derogare de la alineatul (2), un sistem de IA menționat în anexa III nu poate fi considerat ca prezentând un grad ridicat de risc dacă nu prezintă un risc semnificativ de a aduce prejudicii sănătății, siguranței sau drepturilor fundamentale ale persoanelor fizice, inclusiv prin faptul că nu influențează în mod semnificativ rezultatul procesului decizional.

Primul paragraf se aplică în cazul în care oricare dintre următoarele condiții este îndeplinită:

(a) sistemul de IA este destinat să îndeplinească o sarcină procedurală restrânsă;

(b) sistemul de IA este destinat să îmbunătățească rezultatul unei activități umane finalizate anterior;

(c) sistemul de IA este destinat să depisteze modelele decizionale sau abaterile de la modelele decizionale anterioare și nu este menit să înlocuiască sau să influențeze evaluarea umană finalizată anterior, fără o revizuire umană adecvată; sau

(d) sistemul de IA este destinat să îndeplinească o sarcină pregătitoare pentru o evaluare relevantă în scopul cazurilor de utilizare enumerate în anexa III.

În pofida primului paragraf, un sistem de IA menționat în anexa III este întotdeauna considerat ca prezentând un grad ridicat de risc dacă creează profiluri ale persoanelor fizice.

- (4) Orice furnizor care consideră că un sistem de IA menționat în anexa III nu prezintă un grad ridicat de risc documentează evaluarea sa înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune. Furnizorul respectiv este supus obligației de înregistrare prevăzute la articolul 49 alineatul (2). La cererea autorităților naționale competente, furnizorul pune la dispoziție dovezile documentare în sprijinul evaluării.
- (5) După consultarea Consiliului european pentru inteligența artificială (denumit în continuare „Consiliul IA”) și în termen de cel mult ... [18 luni de la data intrării în vigoare a prezentului regulament], Comisia furnizează orientări care precizează modalitățile privind punerea în aplicare practică a prezentului articol, în conformitate cu articolul 96, împreună cu o listă cuprinzătoare de exemple practice de cazuri de utilizare a sistemelor de IA care prezintă un grad ridicat de risc și a celor care nu prezintă un grad ridicat de risc.
- (6) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica alineatul (3) al doilea paragraf de la prezentul articol prin adăugarea de noi condiții față de cele prevăzute la dispoziția menționată sau prin modificarea acestora, în cazul în care există dovezi concrete și fiabile ale existenței unor sisteme de IA care intră în domeniul de aplicare al anexei III, dar care nu prezintă un risc semnificativ de a aduce prejudicii sănătății, siguranței sau drepturilor fundamentale ale persoanelor fizice.

- (7) Comisia adoptă acte delegate în conformitate cu articolul 97 pentru a modifica alineatul (3) al doilea paragraf de la prezentul articol prin eliminarea oricăreia dintre condițiile prevăzute la dispoziția menționată, în cazul în care există dovezi concrete și fiabile că acest lucru este necesar în scopul menținerii nivelului de protecție a sănătății, a siguranței și a drepturilor fundamentale prevăzut în prezentul regulament.
- (8) Orice modificare a condițiilor prevăzute la alineatul (3) al doilea paragraf, adoptată în conformitate cu alineatele (6) și (7) de la prezentul articol, nu reduce nivelul general de protecție a sănătății, a siguranței și a drepturilor fundamentale prevăzut în prezentul regulament și asigură corelarea cu actele delegate adoptate în temeiul articolului 7 alineatul (1) și ține seama de evoluțiile pieței și ale tehnologiei.

Articolul 7

Modificări ale anexei III

- (1) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa III prin adăugarea de cazuri de utilizare a sistemelor de IA cu grad ridicat de risc sau prin modificarea unor astfel de cazuri dacă sunt îndeplinite cumulativ următoarele două condiții:
- (a) sistemele de IA sunt destinate a fi utilizate în oricare dintre domeniile enumerate în anexa III;
 - (b) sistemele de IA prezintă un risc de a aduce prejudicii sănătății și siguranței sau un risc de impact negativ asupra drepturilor fundamentale, iar riscul respectiv este echivalent sau mai mare în raport cu riscul de a aduce prejudicii sau de a provoca un impact negativ prezentat de sistemele de IA cu grad ridicat de risc deja menționate în anexa III.

- (2) Atunci când evaluează condiția prevăzută la alineatul (1) litera (b), Comisia ia în considerare următoarele criterii:
- (a) scopul preconizat al sistemului de IA;
 - (b) măsura în care a fost utilizat sau este probabil să fie utilizat un sistem de IA;
 - (c) natura și volumul datelor prelucrate și utilizate de sistemul de IA, în special dacă sunt prelucrate categorii speciale de date cu caracter personal;
 - (d) măsura în care sistemul de IA acționează în mod autonom și posibilitatea ca o persoană să anuleze o decizie sau recomandări care atrag un potențial prejudiciu;
 - (e) măsura în care utilizarea unui sistem de IA a adus deja prejudicii sănătății și siguranței, a avut un impact negativ asupra drepturilor fundamentale sau a generat motive de îngrijorare semnificative în ceea ce privește probabilitatea unor astfel de prejudicii sau a unui astfel de impact negativ, astfel cum o demonstrează, de exemplu, rapoartele sau acuzațiile documentate prezentate autorităților naționale competente sau alte rapoarte, după caz;
 - (f) amploarea potențială a unor astfel de prejudicii sau a unui astfel de impact negativ, în special în ceea ce privește intensitatea și capacitatea sa de a afecta numeroase persoane sau de a afecta în mod disproporționat un anumit grup de persoane;
 - (g) măsura în care persoanele care sunt potențial prejudiciate sau afectate de un impact negativ depind de rezultatul produs cu ajutorul unui sistem de IA, în special deoarece, din motive practice sau juridice, nu este posibil în mod rezonabil să se renunțe la rezultatul respectiv;

- (h) măsura în care există un dezechilibru de putere sau persoanele care sunt potențial prejudiciate sau afectate de impactul negativ se află într-o poziție vulnerabilă în raport cu implementatorul unui sistem de IA, în special din cauza statutului, a autorității, a cunoștințelor, a circumstanțelor economice sau sociale sau a vârstei;
- (i) măsura în care rezultatul produs cu implicarea unui sistem de IA este ușor de corectat sau reversibil, avându-se în vedere soluțiile tehnice disponibile pentru corectare sau reversare și dat fiind că rezultatele care au un impact negativ asupra sănătății, siguranței sau drepturilor fundamentale nu sunt considerate ca fiind ușor de corectat sau reversibile;
- (j) amploarea și probabilitatea beneficiilor implementării sistemului de IA pentru persoane fizice, grupuri sau societate în general, inclusiv îmbunătățirile posibile ale siguranței produselor;
- (k) măsura în care dreptul existent al Uniunii prevede:
 - (i) măsuri reparatorii eficace în legătură cu riscurile prezentate de un sistem de IA, cu excepția cererilor de despăgubiri;
 - (ii) măsuri eficace de prevenire sau de reducere substanțială a acestor riscuri.

- (3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica lista din anexa III prin eliminarea de sisteme de IA cu grad ridicat de risc în cazul în care sunt îndeplinite cumulativ următoarele două condiții:
- (a) sistemul de IA cu grad ridicat de risc în cauză nu mai prezintă riscuri semnificative pentru drepturile fundamentale, sănătate sau siguranță, ținând seama de criteriile enumerate la alineatul (2);
 - (b) eliminarea nu reduce nivelul general de protecție a sănătății, siguranței și drepturilor fundamentale în temeiul dreptului Uniunii.

SECȚIUNEA 2

CERINȚE PENTRU SISTEMELE DE IA CU GRAD RIDICAT DE RISC

Articolul 8

Respectarea cerințelor

- (1) Sistemele de IA cu grad ridicat de risc respectă cerințele stabilite în prezenta secțiune, ținând seama de scopul lor preconizat, precum și de stadiul de avansare general recunoscut al IA și al tehnologiilor conexe IA. Sistemul de gestionare a riscurilor menționat la articolul 9 este luat în considerare atunci când se asigură respectarea cerințelor respective.

- (2) În cazul în care un produs conține un sistem de IA căruia i se aplică cerințele prezentului regulament, precum și cerințele din legislația de armonizare a Uniunii care figurează în anexa I secțiunea A, furnizorii au responsabilitatea de a se asigura că produsul lor respectă pe deplin toate cerințele aplicabile impuse de legislația aplicabilă de armonizare a Uniunii. Pentru a asigura conformitatea sistemelor de IA cu grad ridicat de risc menționate la alineatul (1) cu cerințele prevăzute în prezenta secțiune și pentru a asigura coerența, a evita suprapunerile și a reduce la minimum sarcinile suplimentare, furnizorii au posibilitatea de a integra, după caz, procesele de testare și raportare necesare, informațiile și documentația pe care le furnizează cu privire la produsul lor în documentația și procedurile deja existente și sunt impuse în temeiul legislației de armonizare a Uniunii care figurează în anexa I secțiunea A.

Articolul 9

Sistemul de gestionare a riscurilor

- (1) Se instituie, se pune în aplicare, se documentează și se menține un sistem de gestionare a riscurilor în legătură cu sistemele de IA cu grad ridicat de risc.
- (2) Sistemul de gestionare a riscurilor este înțeles ca un proces iterativ continuu planificat și derulat pe parcursul întregului ciclu de viață al unui sistem de IA cu grad ridicat de risc, necesitând în mod periodic actualizarea și revizuirea sistematică. Acesta cuprinde următoarele etape:
- (a) identificarea și analiza riscurilor cunoscute și previzibile în mod rezonabil pe care sistemul de IA cu grad ridicat de risc le poate prezenta pentru sănătate, siguranță sau drepturile fundamentale atunci când sistemul de IA cu grad ridicat de risc este utilizat în conformitate cu scopul preconizat;

- (b) estimarea și evaluarea riscurilor care pot apărea atunci când sistemul de IA cu grad ridicat de risc este utilizat în conformitate cu scopul său preconizat și în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil;
 - (c) evaluarea altor riscuri care ar putea apărea pe baza analizei datelor colectate din sistemul de monitorizare ulterioară introducerii pe piață menționat la articolul 72;
 - (d) adoptarea unor măsuri adecvate și specifice de gestionare a riscurilor, concepute pentru a combate riscurile identificate în temeiul literei (a).
- (3) Prezentul articol se referă numai la riscurile care pot fi atenuate sau eliminate în mod rezonabil prin dezvoltarea sau proiectarea sistemului de IA cu grad ridicat de risc sau prin furnizarea de informații tehnice adecvate.
- (4) Măsurile de gestionare a riscurilor menționate la alineatul (2) litera (d) țin seama în mod corespunzător de efectele și interacțiunea posibilă care rezultă din aplicarea combinată a cerințelor prevăzute în prezenta secțiune, în vederea reducerii la minimum a riscurilor într-un mod mai eficace, obținându-se totodată un echilibru adecvat în punerea în aplicare a măsurilor de îndeplinire a cerințelor respective.
- (5) Măsurile de gestionare a riscurilor menționate la alineatul (2) litera (d) sunt de așa natură încât riscul rezidual relevant asociat fiecărui pericol, precum și riscul rezidual global al sistemelor de IA cu grad ridicat de risc să fie considerate a fi acceptabile.

La identificarea celor mai adecvate măsuri de gestionare a riscurilor se asigură următoarele:

- (a) eliminarea sau reducerea riscurilor identificate și evaluate în temeiul alineatului (2), în măsura în care acest lucru este fezabil din punct de vedere tehnic prin proiectarea și dezvoltarea adecvată a sistemului de IA cu grad ridicat de risc;
- (b) după caz, punerea în aplicare a unor măsuri adecvate de atenuare și control pentru combaterea riscurilor care nu pot fi eliminate;
- (c) furnizarea informațiilor necesare în temeiul articolului 13 și, după caz, formarea implementatorilor.

În vederea eliminării sau reducerii riscurilor legate de utilizarea sistemului de IA cu grad ridicat de risc se acordă atenția cuvenită cunoștințelor tehnice, experienței, educației și formării preconizate din partea implementatorului, precum și contextului prezumtiv în care urmează să fie utilizat sistemul.

- (6) Sistemele de IA cu grad ridicat de risc sunt testate în scopul identificării celor mai adecvate măsuri specifice de gestionare a riscurilor. Testarea asigură faptul că sistemele de IA cu grad ridicat de risc funcționează într-un mod coerent cu scopul preconizat și că sunt conforme cu cerințele stabilite în prezenta secțiune.
- (7) Procedurile de testare pot include testarea în condiții reale, în conformitate cu articolul 60.

- (8) Testarea sistemelor de IA cu grad ridicat de risc se efectuează, după caz, în orice moment pe parcursul procesului de dezvoltare și, în orice caz, înainte de introducerea pe piață sau de punerea în funcțiune a acestora. Testarea se efectuează pe baza unor indicatori și a unor praguri probabilistice definite în prealabil, care sunt adecvate scopului preconizat al sistemului de IA cu grad ridicat de risc.
- (9) La punerea în aplicare a sistemului de gestionare a riscurilor descris la alineatele (1)-(7), furnizorii analizează dacă, având în vedere scopul său preconizat, sistemul de IA cu grad ridicat de risc este susceptibil să aibă un impact negativ asupra persoanelor cu vârsta sub 18 ani și, după caz, asupra altor grupuri vulnerabile.
- (10) Pentru furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor cerințe privind procesele interne de gestionare a riscurilor în temeiul altor dispoziții relevante din dreptul Uniunii, aspectele descrise la alineatele (1)-(9) pot face parte din procedurile de gestionare a riscurilor stabilite în temeiul legislației respective sau pot fi combinate cu acestea.

Articolul 10

Datele și guvernarea datelor

- (1) Sistemele de IA cu grad ridicat de risc care utilizează tehnici ce implică antrenarea de modele de IA cu date se dezvoltă pe baza unor seturi de date de antrenament, de validare și de testare care îndeplinesc criteriile de calitate menționate la alineatele (2)-(5) ori de câte ori sunt utilizate astfel de seturi de date.

- (2) Seturile de date de antrenament, de validare și de testare fac obiectul unor practici de guvernanță și gestionare a datelor adecvate scopului preconizat al sistemului de IA cu grad ridicat de risc. Practicile respective se referă în special la:
- (a) opțiunile de proiectare relevante;
 - (b) procesele de colectare a datelor și originea datelor, iar în cazul datelor cu caracter personal, scopul inițial al colectării datelor;
 - (c) operațiunile relevante de prelucrare în vederea pregătirii datelor, cum ar fi adnotarea, etichetarea, curățarea, actualizarea, îmbogățirea și agregarea;
 - (d) formularea unor ipoteze, în special în ceea ce privește informațiile pe care datele ar trebui să le măsoare și să le reprezinte;
 - (e) o evaluare a disponibilității, a cantității și a adecvării seturilor de date necesare;
 - (f) examinarea în vederea identificării unor posibile prejudecăți care sunt susceptibile să afecteze sănătatea și siguranța persoanelor, să aibă un impact negativ asupra drepturilor fundamentale sau să conducă la o discriminare interzisă în temeiul dreptului Uniunii, în special în cazul în care datele de ieșire influențează datele de intrare pentru operațiunile viitoare;
 - (g) măsuri adecvate pentru detectarea, prevenirea și atenuarea posibilelor prejudecăți identificate în conformitate cu litera (f);
 - (h) identificarea lacunelor sau a deficiențelor relevante în materie de date care împiedică conformitatea cu prezentul regulament și a modului în care acestea pot fi abordate.

- (3) Seturile de date de antrenament, de validare și de testare sunt relevante, suficient de reprezentative, și pe cât posibil, fără erori și complete, având în vedere scopul preconizat. Acestea au proprietățile statistice corespunzătoare, inclusiv, după caz, în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul de IA cu grad ridicat de risc. Caracteristicile respective ale seturilor de date pot fi îndeplinite la nivelul seturilor de date individuale sau la nivelul unei combinații a acestora.
- (4) Seturile de date iau în considerare, în măsura impusă de scopul preconizat, caracteristicile sau elementele specifice cadrului geografic, contextual, comportamental sau funcțional specific în care este destinat să fie utilizat sistemul de IA cu grad ridicat de risc.
- (5) În măsura în care acest lucru este strict necesar pentru a asigura detectarea și corectarea prejudecăților în legătură cu sistemele de IA cu grad ridicat de risc în conformitate cu alineatul (2) literele (f) și (g) de la prezentul articol, furnizorii de astfel de sisteme pot prelucra în mod excepțional categoriile speciale de date cu caracter personal, sub rezerva unor garanții adecvate pentru drepturile și libertățile fundamentale ale persoanelor fizice. În plus față de dispozițiile prevăzute de Regulamentele (UE) 2016/679 și (UE) 2018/1725 și de Directiva (UE) 2016/680, pentru ca o astfel de prelucrare să aibă loc, trebuie să fie respectate toate condițiile următoare:
- (a) depistarea și corectarea prejudecăților nu poate fi realizată în mod eficace prin prelucrarea altor date, inclusiv a datelor sintetice sau anonimizate;

- (b) categoriile speciale de date cu caracter personal fac obiectul unor limitări tehnice privind reutilizarea datelor cu caracter personal și al unor măsuri avansate de securitate și de protecție a vieții private, inclusiv pseudonimizarea;
 - (c) categoriile speciale de date cu caracter personal fac obiectul unor măsuri prin care să se asigure că datele cu caracter personal prelucrate sunt securizate și protejate, sub rezerva unor garanții adecvate, inclusiv controale stricte și documentarea accesului, pentru a se evita utilizarea necorespunzătoare și pentru a se asigura că numai persoanele autorizate cu obligații de confidențialitate corespunzătoare au acces la aceste date cu caracter personal;
 - (d) categoriile speciale de date cu caracter personal nu trebuie să fie transmise, transferate sau accesate în alt mod de către alte părți;
 - (e) categoriile speciale de date cu caracter personal sunt șterse după corectarea prejudecăților sau după ce datele cu caracter personal au ajuns la sfârșitul perioadei lor de păstrare, în funcție de care dintre acestea survine mai întâi;
 - (f) evidențele activităților de prelucrare în temeiul Regulamentelor (UE) 2016/679 și (UE) 2018/1725 și al Directivei (UE) 2016/680 includ motivele pentru care a fost strict necesară prelucrarea unor categorii speciale de date cu caracter personal pentru a depista și a corecta prejudecățile și motivele pentru care acest obiectiv nu putea fi realizat prin prelucrarea altor date.
- (6) Pentru dezvoltarea sistemelor de IA cu grad ridicat de risc care nu utilizează tehnici care implică antrenarea de modele de IA, alineatele (2)-(5) se aplică numai seturilor de date de testare.

Articolul 11
Documentația tehnică

- (1) Documentația tehnică a unui sistem de IA cu grad ridicat de risc se întocmește înainte ca sistemul respectiv să fie introdus pe piață sau pus în funcțiune și se actualizează.

Documentația tehnică se întocmește astfel încât să demonstreze că sistemul de IA cu grad ridicat de risc respectă cerințele prevăzute în prezenta secțiune și să furnizeze autorităților naționale competente și organismelor notificate informațiile necesare într-un mod clar și cuprinzător, pentru a evalua conformitatea sistemului de IA cu cerințele respective.

Aceasta conține cel puțin elementele prevăzute în anexa IV. IMM-urile, inclusiv întreprinderile nou-înființate, pot furniza într-o manieră simplificată elementele documentației tehnice specificate în anexa IV. În acest scop, Comisia stabilește un formular simplificat de documentație tehnică care vizează nevoile întreprinderilor mici și ale microîntreprinderilor. În cazul în care IMM-urile, inclusiv întreprinderile nou-înființate, optează să furnizeze informațiile solicitate în anexa IV într-o manieră simplificată, acestea utilizează formularul menționat la prezentul alineat. Organismele notificate acceptă formularul în scopul evaluării conformității.

- (2) În cazul în care este introdus pe piață sau pus în funcțiune un sistem de IA cu grad ridicat de risc legat de un produs care face obiectul actelor legislative de armonizare ale Uniunii care figurează în anexa I secțiunea A, se întocmește o singură documentație tehnică ce conține toate informațiile prevăzute la alineatul (1), precum și informațiile necesare în temeiul respectivelor acte juridice.

- (3) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa IV, atunci când este necesar, pentru a se asigura că, având în vedere progresul tehnic, documentația tehnică furnizează toate informațiile necesare pentru evaluarea conformității sistemului cu cerințele prevăzute în prezenta secțiune.

Articolul 12

Păstrarea evidențelor

- (1) Sistemele de IA cu grad ridicat de risc permit din punct de vedere tehnic înregistrarea automată a evenimentelor (fișiere de jurnalizare) de-a lungul duratei de viață a sistemului.
- (2) Pentru a asigura un nivel de trasabilitate a funcționării sistemului de IA cu grad ridicat de risc care să fie adecvat scopului preconizat al sistemului, capabilitățile de jurnalizare permit înregistrarea evenimentelor relevante pentru:
- (a) identificarea situațiilor care pot avea ca rezultat faptul că sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1) sau care pot conduce la o modificare substanțială;
 - (b) facilitarea monitorizării ulterioare introducerii pe piață menționate la articolul 72; și
 - (c) monitorizarea funcționării sistemelor de IA cu grad ridicat de risc menționate la articolul 26 alineatul (5).
- (3) În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 1 litera (a), capabilitățile de jurnalizare furnizează cel puțin:
- (a) înregistrarea perioadei fiecărei utilizări a sistemului (data și ora de începere, precum și data și ora de încheiere a fiecărei utilizări);

- (b) baza de date de referință în raport cu care au fost verificate de sistem datele de intrare;
- (c) datele de intrare pentru care căutarea a generat o concordanță;
- (d) identificarea persoanelor fizice implicate în verificarea rezultatelor, astfel cum se menționează la articolul 14 alineatul (5).

Articolul 13

Transparența și furnizarea de informații implementatorilor

- (1) Sistemele de IA cu grad ridicat de risc sunt proiectate și dezvoltate astfel încât să se asigure că funcționarea lor este suficient de transparentă pentru a permite implementatorilor să interpreteze rezultatele sistemului și să le utilizeze în mod corespunzător. Se asigură un tip și un grad adecvat de transparență, în vederea respectării obligațiilor relevante ale furnizorului și ale implementatorului prevăzute în secțiunea 3.
- (2) Sistemele de IA cu grad ridicat de risc sunt însoțite de instrucțiuni de utilizare într-un format digital adecvat sau în alt tip de format adecvat, care includ informații concise, complete, corecte și clare care sunt relevante, accesibile și ușor de înțeles pentru implementatori.
- (3) Instrucțiunile de utilizare conțin cel puțin următoarele informații:
 - (a) identitatea și datele de contact ale furnizorului și, după caz, ale reprezentantului său autorizat;

- (b) caracteristicile, capacitățile și limitările performanței sistemului de IA cu grad ridicat de risc, inclusiv:
- (i) scopul său preconizat;
 - (ii) nivelul de acuratețe, inclusiv indicatorii săi, de robustețe și de securitate cibernetică menționat la articolul 15 în raport cu care sistemul de IA cu grad ridicat de risc a fost testat și validat și care poate fi preconizat, precum și orice circumstanță cunoscută și previzibilă care ar putea avea un impact asupra nivelului preconizat de acuratețe, robustețe și securitate cibernetică;
 - (iii) orice circumstanță cunoscută sau previzibilă legată de utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu scopul său preconizat sau în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil, care poate conduce la riscurile pentru sănătate și siguranță sau pentru drepturile fundamentale menționate la articolul 9 alineatul (2);
 - (iv) după caz, capacitățile și caracteristicile tehnice ale sistemului de IA cu grad ridicat de risc de a furniza informații relevante pentru explicarea rezultatelor sale;
 - (v) după caz, performanțele sale în ceea ce privește anumite persoane sau grupuri de persoane în legătură cu care este destinat să fie utilizat sistemul;
 - (vi) după caz, specificațiile pentru datele de intrare sau orice altă informație relevantă în ceea ce privește seturile de date de antrenament, de validare și de testare utilizate, ținând seama de scopul preconizat al sistemului de IA cu grad ridicat de risc;

- (vii) după caz, informații care să le permită implementatorilor să interpreteze rezultatele sistemului de IA cu grad ridicat de risc și să le utilizeze în mod corespunzător;
- (c) modificările aduse sistemului de IA cu grad ridicat de risc și performanței acestuia care au fost determinate de către furnizor la momentul evaluării inițiale a conformității, dacă este cazul;
- (d) măsurile de supraveghere umană menționate la articolul 14, inclusiv măsurile tehnice instituite pentru a facilita interpretarea rezultatelor sistemelor de IA cu grad ridicat de risc de către implementatori;
- (e) resursele de calcul și resursele hardware necesare, durata de viață preconizată a sistemului de IA cu grad ridicat de risc și orice măsuri de întreținere și de îngrijire, inclusiv frecvența lor, necesare pentru a asigura funcționarea corespunzătoare a sistemului de IA respectiv, inclusiv în ceea ce privește actualizările software-ului;
- (f) după caz, o descriere a mecanismelor incluse în sistemul de IA cu grad ridicat de risc care să permită implementatorilor să colecteze, să stocheze și să interpreteze în mod corespunzător fișierele de jurnalizare în conformitate cu articolul 12.

Articolul 14

Supravegherea umană

- (1) Sistemele de IA cu grad ridicat de risc sunt proiectate și dezvoltate astfel încât, prin includerea de instrumente adecvate de interfață om-mașină, să poată fi supravegheate în mod eficace de către persoane fizice în perioada în care sunt utilizate.

- (2) Supravegherea umană are ca scop prevenirea sau reducerea la minimum a riscurilor pentru sănătate, siguranță sau pentru drepturile fundamentale, care pot apărea atunci când un sistem de IA cu grad ridicat de risc este utilizat în conformitate cu scopul său preconizat sau în condiții de utilizare necorespunzătoare previzibilă în mod rezonabil, în special în cazurile în care astfel de riscuri persistă în pofida aplicării altor cerințe prevăzute în prezenta secțiune.
- (3) Măsurile de supraveghere sunt proporționale cu riscurile specifice, cu nivelul de autonomie și cu contextul utilizării sistemului de IA cu grad ridicat de risc și se asigură fie prin unul dintre următoarele tipuri de măsuri, fie prin ambele:
- (a) măsuri identificate și încorporate, atunci când este fezabil din punct de vedere tehnic, în sistemul de IA cu grad ridicat de risc de către furnizor înainte ca acesta să fie introdus pe piață sau pus în funcțiune;
 - (b) măsuri identificate de furnizor înainte de introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc și care sunt adecvate pentru a fi puse în aplicare de implementator.
- (4) În scopul punerii în aplicare a alineatelor (1), (2) și (3), sistemul de IA cu grad ridicat de risc este pus la dispoziția implementatorului astfel încât persoanelor fizice cărora li se încredințează supravegherea umană să li se permită, în funcție de următoarele și proporțional cu acestea:
- (a) să înțeleagă în mod corespunzător capacitățile și limitările relevante ale sistemului de IA cu grad ridicat de risc și să fie în măsură să monitorizeze în mod corespunzător funcționarea acestuia, inclusiv în vederea depistării și abordării anomaliilor, disfuncționalităților și performanțelor neașteptate;

- (b) să rămână conștiente de posibila tendință de a se baza în mod automat sau excesiv pe rezultatele obținute de un sistem de IA cu grad ridicat de risc (prejudecăți legate de automatizare), în special în cazul sistemelor de IA cu grad ridicat de risc utilizate pentru a furniza informații sau recomandări pentru deciziile care urmează să fie luate de persoanele fizice;
 - (c) să interpreteze corect rezultatele sistemului de IA cu grad ridicat de risc, ținând seama, de exemplu, de instrumentele și metodele de interpretare disponibile;
 - (d) să decidă, în orice situație anume, să nu utilizeze sistemul de IA cu grad ridicat de risc sau să ignore, să anuleze sau să inverseze rezultatele sistemului de IA cu grad ridicat de risc;
 - (e) să intervină în funcționarea sistemului de IA cu grad ridicat de risc sau să întrerupă sistemul prin intermediul unui buton „stop” sau al unei proceduri similare care să permită sistemului să se oprească în condiții de siguranță.
- (5) În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 1 litera (a), măsurile menționate la alineatul (3) de la prezentul articol sunt de așa natură încât să asigure că, în plus, implementatorul nu ia nicio măsură sau decizie pe baza identificării care rezultă din sistem, cu excepția cazului în care identificarea respectivă a fost verificată și confirmată separat de cel puțin două persoane fizice care au competența, pregătirea și autoritatea necesare.

Cerința unei verificări separate de către cel puțin două persoane fizice nu se aplică sistemelor de IA cu grad ridicat de risc utilizate în scopul aplicării legii sau în domeniul imigrației, al controlului la frontiere ori al azilului, în cazurile în care dreptul Uniunii sau dreptul intern consideră că aplicarea acestei cerințe este disproporționată.

Articolul 15

Acuratețe, robustețe și securitate cibernetică

- (1) Sistemele de IA cu grad ridicat de risc sunt concepute și dezvoltate astfel încât să atingă un nivel adecvat de acuratețe, robustețe și securitate cibernetică și să funcționeze în mod consecvent în aceste privințe pe parcursul întregului lor ciclu de viață.
- (2) Pentru a aborda aspectele tehnice ale modului de măsurare a nivelurilor adecvate de acuratețe și robustețe prevăzute la alineatul (1) și orice alți indicatori de performanță relevanți, Comisia, în cooperare cu părți interesate și organizații relevante precum autoritățile din domeniul metrologiei și al etalonării încurajează, după caz, elaborarea de valori de referință și metodologii de măsurare.
- (3) Nivelurile de acuratețe și indicatorii de acuratețe relevanți ai sistemelor de IA cu grad ridicat de risc se declară în instrucțiunile de utilizare aferente.
- (4) Sistemele de IA cu grad ridicat de risc sunt cât mai reziliente posibil în ceea ce privește erorile, defecțiunile sau incoerențele care pot apărea în cadrul sistemului sau în mediul în care funcționează sistemul, în special din cauza interacțiunii lor cu persoane fizice sau cu alte sisteme. Se iau măsuri tehnice și organizatorice în acest sens.

Robustețea sistemelor de IA cu grad ridicat de risc poate fi asigurată prin soluții tehnice redundante, care pot include planuri de rezervă sau de funcționare în caz de avarie.

Sistemele de IA cu grad ridicat de risc care continuă să învețe după ce au fost introduse pe piață sau puse în funcțiune sunt dezvoltate astfel încât să elimine sau să reducă pe cât posibil riscul ca eventuale rezultate distorsionate de prejudecăți să influențeze datele de intrare pentru operațiunile viitoare (bucle de feedback) și să se asigure că orice astfel de bucle de feedback sunt abordate în mod corespunzător prin măsuri de atenuare adecvate.

- (5) Sistemele de IA cu grad ridicat de risc sunt reziliente în ceea ce privește încercările unor părți terțe neautorizate de a le modifica utilizarea, rezultatele sau performanța prin exploatarea vulnerabilităților sistemului.

Soluțiile tehnice menite să asigure securitatea cibernetică a sistemelor de IA cu grad ridicat de risc sunt adecvate circumstanțelor relevante și riscurilor.

Soluțiile tehnice pentru abordarea vulnerabilităților specifice ale IA includ, după caz, măsuri de prevenire, depistare, răspuns, soluționare și control în privința atacurilor ce vizează manipularea setului de date de antrenament (otrăvirea datelor) sau a componentelor preantrenate utilizate la antrenament (otrăvirea modelelor), a datelor de intrare concepute să determine modelul de IA să facă o greșeală (exemple contradictorii sau eludarea modelelor), a atacurilor la adresa confidențialității sau a defectelor modelului.

SECȚIUNEA 3
OBLIGAȚIILE FURNIZORILOR ȘI IMPLEMENTATORILOR DE SISTEME DE IA
CU GRAD RIDICAT DE RISC ȘI ALE ALTOR PĂRȚI

Articolul 16

Obligațiile furnizorilor de sisteme de IA cu grad ridicat de risc

Furnizorii de sisteme de IA cu grad ridicat de risc:

- (a) se asigură că sistemele lor de IA cu grad ridicat de risc respectă cerințele prevăzute în secțiunea 2;
- (b) indică pe sistemul de IA cu grad ridicat de risc sau, în cazul în care acest lucru nu este posibil, pe ambalaj sau în documentele care îl însoțesc, după caz, numele lor, denumirea lor comercială înregistrată sau marca lor înregistrată, adresa la care pot fi contactați;
- (c) dispun de un sistem de management al calității în conformitate cu articolul 17;
- (d) păstrează documentația menționată la articolul 18;
- (e) atunci când acestea se află sub controlul lor, păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc menționate la articolul 19;
- (f) se asigură că sistemul de IA cu grad ridicat de risc este supus procedurii relevante de evaluare a conformității menționată la articolul 43, înainte de introducerea sa pe piață sau de punerea sa în funcțiune;

- (g) elaborează o declarație de conformitate UE în conformitate cu articolul 47;
- (h) aplică marcajul CE pe sistemul de IA cu grad ridicat de risc sau, în cazul în care acest lucru nu este posibil, pe ambalajul sau în documentația sa însoțitoare, pentru a indica conformitatea cu prezentul regulament, în conformitate cu articolul 48;
- (i) respectă obligațiile de înregistrare menționate la articolul 49 alineatul (1);
- (j) iau măsurile corective necesare și furnizează informațiile prevăzute la articolul 20;
- (k) la cererea motivată a unei autorități naționale competente, demonstrează conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2;
- (l) se asigură că sistemul de IA cu grad ridicat de risc respectă cerințele de accesibilitate, în conformitate cu Directivele (UE) 2016/2102 și (UE) 2019/882.

Articolul 17

Sistemul de management al calității

- (1) Furnizorii de sisteme de IA cu grad ridicat de risc instituie un sistem de management al calității care asigură conformitatea cu prezentul regulament. Acest sistem este documentat în mod sistematic și ordonat sub formă de politici, proceduri și instrucțiuni scrise și include cel puțin următoarele aspecte:
 - (a) o strategie pentru conformitatea cu reglementările, inclusiv conformitatea cu procedurile de evaluare a conformității și cu procedurile de gestionare a modificărilor aduse sistemului de IA cu grad ridicat de risc;

- (b) tehnicile, procedurile și acțiunile sistematice care trebuie utilizate pentru proiectarea, controlul proiectării și verificarea proiectării sistemului de IA cu grad ridicat de risc;
- (c) tehnicile, procedurile și acțiunile sistematice care trebuie utilizate pentru dezvoltarea, controlul calității și asigurarea calității sistemului de IA cu grad ridicat de risc;
- (d) procedurile de examinare, testare și validare care trebuie efectuate înainte, în timpul și după dezvoltarea sistemului de IA cu grad ridicat de risc, precum și frecvența cu care acestea trebuie efectuate;
- (e) specificațiile tehnice, inclusiv standardele, care trebuie aplicate și, în cazul în care standardele armonizate relevante nu sunt aplicate integral sau nu vizează toate cerințele relevante prevăzute în secțiunea 2, mijloacele care trebuie utilizate pentru a se asigura că sistemul de IA cu grad ridicat de risc respectă cerințele respective;
- (f) sisteme și proceduri pentru gestionarea datelor, inclusiv obținerea datelor, colectarea datelor, analiza datelor, etichetarea datelor, stocarea datelor, filtrarea datelor, extragerea datelor, agregarea datelor, păstrarea datelor și orice altă operațiune privind datele care este efectuată înainte și în scopul introducerii pe piață sau al punerii în funcțiune a sistemelor de IA cu grad ridicat de risc;
- (g) sistemul de gestionare a riscurilor menționat la articolul 9;
- (h) instituirea, implementarea și întreținerea unui sistem de monitorizare ulterioară introducerii pe piață, în conformitate cu articolul 72;

- (i) procedurile legate de raportarea unui incident grav în conformitate cu articolul 73;
 - (j) gestionarea comunicării cu autoritățile naționale competente, cu alte autorități relevante, inclusiv cu cele care furnizează sau sprijină accesul la date, cu organismele notificate, cu alți operatori, cu clienți sau cu alte părți interesate;
 - (k) sisteme și proceduri pentru păstrarea evidențelor tuturor documentelor și informațiilor relevante;
 - (l) gestionarea resurselor, inclusiv măsurile legate de securitatea aprovizionării;
 - (m) un cadru de asigurare a răspunderii care stabilește responsabilitățile cadrelor de conducere și ale altor categorii de personal în ceea ce privește toate aspectele enumerate la prezentul alineat.
- (2) Punerea în aplicare a aspectelor menționate la alineatul (1) este proporțională cu dimensiunea organizației furnizorului. Furnizorii respectă, indiferent de situație, gradul de precizie și nivelul de protecție necesare pentru a asigura conformitatea cu prezentul regulament a sistemelor lor de IA cu grad ridicat de risc.
- (3) Furnizorii de sisteme de IA cu grad ridicat de risc care fac obiectul unor obligații în ceea ce privește sistemele de management al calității sau o funcție echivalentă a acestora în temeiul dreptului sectorial relevant al Uniunii pot include aspectele descrise la alineatul (1) ca parte din sistemele de management al calității stabilite în temeiul dreptului respectiv.

- (4) În cazul furnizorilor care sunt instituții financiare supuse unor cerințe privind guvernanta internă, măsurile sau procesele interne în temeiul dreptului Uniunii din domeniul serviciilor financiare, se consideră că obligația de instituire a unui sistem de management al calității, cu excepția alineatului (1) literele (g), (h) și (i) de la prezentul articol, este îndeplinită prin respectarea normelor privind măsurile sau procesele de guvernanta internă în temeiul dreptului relevant al Uniunii din domeniul serviciilor financiare. În acest scop, se ține seama de toate standardele armonizate menționate la articolul 40.

Articolul 18

Păstrarea evidențelor

- (1) Pentru o perioadă de 10 ani după introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc, furnizorul păstrează la dispoziția autorităților naționale competente:
- (a) documentația tehnică menționată la articolul 11;
 - (b) documentația privind sistemul de management al calității menționată la articolul 17;
 - (c) documentația privind modificările aprobate de organismele notificate, după caz;
 - (d) deciziile și alte documente emise de organismele notificate, după caz;
 - (e) declarația de conformitate UE prevăzută la articolul 47.

- (2) Fiecare stat membru stabilește condițiile în care documentația menționată la alineatul (1) rămâne la dispoziția autorităților naționale competente pentru perioada indicată la alineatul respectiv pentru cazurile în care un furnizor sau reprezentantul autorizat al acestuia stabilit pe teritoriul său intră în faliment sau își încetează activitatea înainte de sfârșitul perioadei respective.
- (3) Furnizorii care sunt instituții financiare supuse unor cerințe privind guvernanța internă, măsurile sau procesele lor interne în temeiul dreptului Uniunii din domeniul serviciilor financiare păstrează documentația tehnică ca parte a documentației păstrate în temeiul dreptului relevant al Uniunii din domeniul serviciilor financiare.

Articolul 19

Fișiere de jurnalizare generate automat

- (1) Furnizorii de sisteme de IA cu grad ridicat de risc păstrează fișierele de jurnalizare menționate la articolul 12 alineatul (1), generate automat de sistemele de IA cu grad ridicat de risc ale acestora, în măsura în care astfel de fișiere de jurnalizare se află sub controlul lor. Fără a aduce atingere dreptului Uniunii sau dreptului intern aplicabil, fișiere de jurnalizare se păstrează pentru o perioadă adecvată scopului preconizat al sistemului de IA cu grad ridicat de risc, de cel puțin șase luni, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul intern aplicabil, în special în dreptul Uniunii privind protecția datelor cu caracter personal.
- (2) Furnizorii care sunt instituții financiare supuse unor cerințe privind guvernanța lor internă, măsurile sau procesele lor interne în temeiul dreptului Uniunii din domeniul serviciilor financiare păstrează fișierele de jurnalizare generate automat de sistemele lor de IA cu grad ridicat de risc ca parte a documentației păstrate în temeiul dreptului relevant din domeniul serviciilor financiare.

Articolul 20

Măsuri corective și obligația de informare

- (1) Furnizorii de sisteme de IA cu grad ridicat de risc care consideră sau au motive să considere că un sistem de IA cu grad ridicat de risc pe care l-au introdus pe piață ori pe care l-au pus în funcțiune nu este în conformitate cu prezentul regulament întreprind imediat măsurile corective necesare pentru ca sistemul să fie adus în conformitate sau să fie retras, dezactivat sau rechemat, după caz. Aceștia informează în acest sens distribuitorii sistemului de IA cu grad ridicat de risc în cauză și, dacă este cazul, implementatorii, reprezentantul autorizat și importatorii.
- (2) În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1), iar furnizorul ia cunoștință de riscul respectiv, acesta investighează imediat cauzele, în colaborare cu implementatorul care efectuează raportarea, după caz, și informează autoritățile de supraveghere a pieței competente pentru sistemul de IA cu grad ridicat de risc în cauză și, după caz, organismul notificat care a eliberat un certificat pentru sistemul de IA cu grad ridicat de risc respectiv în conformitate cu articolul 44, în special cu privire la natura neconformității și la orice măsură corectivă relevantă întreprinsă.

Articolul 21

Cooperarea cu autoritățile competente

- (1) La cererea motivată a unei autorități competente, furnizorii de sisteme de IA cu grad ridicat de risc furnizează autorității respective toate informațiile și documentația necesare pentru a demonstra conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, într-o limbă care poate fi ușor înțeleasă de către autoritatea respectivă și care este una dintre limbile oficiale ale instituțiilor Uniunii, astfel cum sunt indicate de statul membru în cauză.
- (2) La cererea motivată a unei autorități competente, furnizorii acordă, de asemenea, autorității competente solicitante, după caz, acces la fișierele de jurnalizare generate automat ale sistemului de IA cu grad ridicat de risc menționate la articolul 12 alineatul (1), în măsura în care respectivele fișiere de jurnalizare se află sub controlul lor.
- (3) Toate informațiile obținute de autoritățile competente în temeiul prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 22

Reprezentanții autorizați ai furnizorilor de sisteme de IA cu grad ridicat de risc

- (1) Înainte de a-și pune la dispoziție sistemele de IA cu grad ridicat de risc pe piața Uniunii, furnizorii stabiliți în țări terțe desemnează, prin mandat scris, un reprezentant autorizat care este stabilit în Uniune.

- (2) Furnizorul permite reprezentantului său autorizat să îndeplinească sarcinile prevăzute în mandatul primit de la furnizor.
- (3) Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la furnizor. Acesta furnizează autorităților de supraveghere a pieței, la cerere, o copie a mandatului, într-una din limbile oficiale ale instituțiilor Uniunii, astfel cum este indicată de autoritatea competentă. În sensul prezentului regulament, mandatul îl autorizează pe reprezentantul autorizat să îndeplinească următoarele sarcini:
- (a) să verifice dacă au fost întocmite declarația de conformitate UE menționată la articolul 47 și documentația tehnică menționată la articolul 11 și dacă furnizorul a desfășurat o procedură corespunzătoare de evaluare a conformității;
 - (b) să păstreze la dispoziția autorităților competente și a autorităților sau organismelor naționale menționate la articolul 74 alineatul (10), pentru o perioadă de 10 ani de la introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc, datele de contact ale furnizorului care a desemnat reprezentantul autorizat, o copie a declarației de conformitate UE menționată la articolul 47, documentația tehnică și, dacă este cazul, certificatul eliberat de organismul notificat;
 - (c) să furnizeze unei autorități competente, pe baza unei cereri motivate, toate informațiile și documentația, inclusiv cele menționate la litera (b) de la prezentul paragraf, necesare pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, inclusiv accesul la fișierele de jurnalizare, astfel cum sunt menționate la articolul 12 alineatul (1), generate automat de sistemul de IA cu grad ridicat de risc, în măsura în care aceste fișiere de jurnalizare se află sub controlul furnizorului;

- (d) să coopereze cu autoritățile competente, în urma unei cereri motivate, cu privire la orice acțiune întreprinsă de acestea din urmă în legătură cu sistemul de IA cu grad ridicat de risc, în special pentru a reduce și a atenua riscurile prezentate de sistemul de IA cu grad ridicat de risc;
- (e) după caz, să respecte obligațiile de înregistrare menționate la articolul 49 alineatul (1) sau, dacă înregistrarea este efectuată chiar de furnizor, să se asigure că informațiile menționate la secțiunea A punctul 3 din anexa VIII sunt corecte.

Mandatul împuternicește reprezentantul autorizat să fie contactat, în afara sau în locul furnizorului, de către autoritățile competente, cu referire la toate aspectele legate de asigurarea conformității cu prezentul regulament.

- (4) Reprezentantul autorizat își reziliază mandatul dacă consideră sau are motive să considere că furnizorul acționează contrar obligațiilor care îi revin în temeiul prezentului regulament. Într-un astfel de caz, el informează imediat autoritatea relevantă de supraveghere a pieței, precum și, după caz, organismul notificat relevant, cu privire la rezilierea mandatului și la motivele acesteia.

Articolul 23

Obligațiile importatorilor

- (1) Înainte de introducerea pe piață a unui sistem de IA cu grad ridicat de risc, importatorii unui astfel de sistem se asigură că sistemul este în conformitate cu prezentul regulament, verificând dacă:
 - (a) procedura relevantă de evaluare a conformității menționată la articolul 43 a fost efectuată de furnizorul sistemului de IA cu grad ridicat de risc;

- (b) furnizorul a întocmit documentația tehnică în conformitate cu articolul 11 și cu anexa IV;
 - (c) sistemul poartă marcajul CE necesar și este însoțit de declarația de conformitate UE menționată la articolul 47 și de instrucțiunile de utilizare;
 - (d) furnizorul a desemnat un reprezentant autorizat în conformitate cu articolul 22 alineatul (1).
- (2) În cazul în care un importator are suficiente motive să considere că un sistem de IA cu grad ridicat de risc nu este în conformitate cu prezentul regulament, sau este falsificat ori însoțit de o documentație falsificată, acesta nu introduce sistemul respectiv pe piață înainte de a fi adus în conformitate. În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1), importatorul informează în acest sens furnizorul sistemului, reprezentanții autorizați și autoritățile de supraveghere a pieței.
- (3) Importatorii indică numele lor, denumirea lor comercială înregistrată sau marca lor înregistrată și adresa la care pot fi contactați în privința sistemului de IA cu grad ridicat de risc și pe ambalajul acestuia sau în documentele care îl însoțesc, dacă este cazul.
- (4) Importatorii se asigură că, pe întreaga perioadă în care un sistem de IA cu grad ridicat de risc se află în responsabilitatea lor, condițiile de depozitare sau de transport, după caz, nu periclitează conformitatea sa cu cerințele prevăzute în secțiunea 2.

- (5) Importatorii păstrează, timp de 10 ani de la introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc, o copie a certificatului eliberat de organismul notificat, după caz, a instrucțiunilor de utilizare și a declarației de conformitate UE menționată la articolul 47.
- (6) Importatorii furnizează autorităților competente relevante, pe baza unei cereri motivate, toate informațiile și documentația necesare, inclusiv cele menționate la alineatul (5), pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, într-o limbă care poate fi ușor înțeleasă de acestea. În acest scop, aceștia se asigură, de asemenea, că documentația tehnică poate fi pusă la dispoziția autorităților respective.
- (7) Importatorii cooperează cu autoritățile competente relevante cu privire la orice acțiune întreprinsă de autoritățile respective în legătură cu un sistem de IA cu grad ridicat de risc introdus pe piață de importatori, în special pentru a reduce sau a atenua riscurile prezentate de acesta.

Articolul 24

Obligațiile distribuitorilor

- (1) Înainte de a pune la dispoziție pe piață un sistem de IA cu grad ridicat de risc, distribuitorii verifică dacă acesta poartă marcajul CE necesar, dacă este însoțit de o copie a declarației de conformitate UE menționată la articolul 47 și de instrucțiunile de utilizare și dacă furnizorul și importatorul sistemului respectiv, după caz, au respectat obligațiile lor respective prevăzute la articolul 16 literele (b) și (c) și la articolul 23 alineatul (3).

- (2) În cazul în care un distribuitor consideră sau are motive să considere, pe baza informațiilor pe care le deține, că un sistem de IA cu grad ridicat de risc nu este în conformitate cu cerințele prevăzute în secțiunea 2, acesta nu pune la dispoziție pe piață sistemul de IA cu grad ridicat de risc înainte ca sistemul să fie adus în conformitate cu cerințele respective. În plus, în cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1), distribuitorul informează furnizorul sau importatorul sistemului, după caz, în acest sens.
- (3) Distribuitorii se asigură că, atât timp cât un sistem de IA cu grad ridicat de risc se află în responsabilitatea lor, condițiile de depozitare sau de transport, după caz, nu periclitează conformitatea sistemului cu cerințele prevăzute în secțiunea 2.
- (4) Un distribuitor care consideră sau are motive să considere, pe baza informațiilor pe care le deține, că un sistem de IA cu grad ridicat de risc pe care l-a pus la dispoziție pe piață nu este în conformitate cu cerințele prevăzute în secțiunea 2 ia măsurile corective necesare pentru a aduce sistemul în conformitate cu cerințele respective, pentru a-l retrage sau pentru a-l rechema sau se asigură că furnizorul, importatorul sau orice operator relevant, după caz, ia măsurile corective respective. În cazul în care sistemul de IA cu grad ridicat de risc prezintă un risc în sensul articolului 79 alineatul (1), distribuitorul informează imediat în acest sens furnizorul sau importatorul sistemului și autoritățile competente pentru sistemul de IA cu grad ridicat de risc în cauză, oferind informații detaliate, în special despre neconformitate și orice măsură corectivă întreprinsă.

- (5) Pe baza unei cereri motivate a unei autorități competente relevante, distribuitorii unor sisteme de IA cu grad ridicat de risc furnizează autorității respective toate informațiile și documentația referitoare la acțiunile lor în temeiul alineatelor (1)-(4), necesare pentru a demonstra conformitatea respectivelor sisteme cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2.
- (6) Distribuitorii cooperează cu autoritățile competente relevante cu privire la orice acțiune întreprinsă de autoritățile respective în legătură cu un sistem de IA cu grad ridicat de risc pus la dispoziție pe piață de distribuitori, în special pentru a reduce sau a atenua riscul prezentat de acesta.

Articolul 25

Responsabilitățile de-a lungul lanțului valoric al IA

- (1) Se consideră că orice distribuitor, importator, implementator sau altă parte terță este furnizor al unui sistem de IA cu grad ridicat de risc în sensul prezentului regulament și este supus obligațiilor care îi revin furnizorului în temeiul articolului 16, în oricare dintre următoarele situații:
- (a) își aplică numele sau marca comercială pe un sistem de IA cu grad ridicat de risc deja introdus pe piață sau pus în funcțiune, fără a aduce atingere dispozițiilor contractuale care prevăd o repartizare diferită a obligațiilor;
 - (b) modifică substanțial un sistem de IA cu grad ridicat de risc care a fost deja introdus pe piață sau a fost deja pus în funcțiune, astfel încât acesta rămâne un sistem de IA cu grad ridicat de risc în temeiul articolului 6;

- (c) modifică scopul preconizat al un sistem de IA, inclusiv al unui sistem IA de uz general, care nu a fost clasificat ca prezentând un grad ridicat de risc și a fost deja introdus pe piață sau pus în funcțiune, astfel încât sistemul de IA în cauză devine un sistem IA cu grad ridicat de risc în conformitate cu articolul 6.
- (2) În cazul în care se produc circumstanțele menționate la alineatul (1), furnizorul care a introdus inițial pe piață sau a pus în funcțiune sistemul de IA nu mai este considerat furnizorul respectivului sistem de IA în sensul prezentului regulament. Acest furnizor inițial cooperează îndeaproape cu noii furnizori și pune la dispoziție informațiile necesare și oferă accesul tehnic și alte tipuri de asistență preconizate în mod rezonabil care sunt necesare pentru îndeplinirea obligațiilor prevăzute în prezentul regulament, în special în ceea ce privește respectarea cerințelor privind evaluarea conformității sistemelor de IA cu grad ridicat de risc. Prezentul alineat nu se aplică în cazurile în care furnizorul inițial a specificat în mod clar că sistemul său de IA nu trebuie transformat într-un sistem de IA cu grad ridicat de risc și, prin urmare, nu intră sub incidența obligației de a preda documentația.
- (3) În cazul sistemelor de IA cu grad ridicat de risc care sunt componente de siguranță ale unor produse cărora li se aplică actele legislative de armonizare ale Uniunii care figurează în anexa I secțiunea A, fabricantul produselor respective este considerat furnizorul sistemului de IA cu grad ridicat de risc și este supus obligațiilor menționate la articolul 16 în oricare dintre următoarele situații:
- (a) sistemul de IA cu grad ridicat de risc este introdus pe piață împreună cu produsul sub numele sau marca comercială a fabricantului produsului;
- (b) sistemul de IA cu grad ridicat de risc este pus în funcțiune sub numele sau marca comercială a fabricantului produsului după ce produsul a fost introdus pe piață.

- (4) Furnizorul unui sistem de IA cu grad ridicat de risc și partea terță care furnizează un sistem de IA, instrumente, servicii, componente sau procese care sunt utilizate sau integrate într-un sistem de IA cu grad ridicat de risc specifică, printr-un acord scris, pe baza stadiului de avansare general recunoscut al tehnologiei, informațiile, capacitățile, accesul tehnic și alte tipuri de asistență necesare pentru a permite furnizorului sistemului de IA cu grad ridicat de risc să respecte întru totul obligațiile prevăzute în prezentul regulament. Prezentul alineat nu se aplică terților care pun la dispoziția publicului instrumente, servicii, procese sau componente, în afara modelelor de IA de uz general, sub licență liberă și deschisă.

Oficiul pentru IA poate elabora și recomanda un model voluntar de clauze pentru contractele dintre furnizorii de sisteme de IA cu grad ridicat de risc și părțile terțe care furnizează instrumente, servicii, componente sau procese care sunt utilizate sau integrate în sistemele de IA cu grad ridicat de risc. Atunci când elaborează modelul voluntar de clauze, Oficiul pentru IA ia în considerare eventualele cerințe contractuale aplicabile în anumite sectoare sau situații economice. Modelul voluntar de clauze se publică și este disponibil gratuit într-un format electronic ușor de utilizat.

- (5) Alineatele (2) și (3) nu aduc atingere necesității de a respecta și de a proteja drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale în conformitate cu dreptul Uniunii și cu dreptul intern.

Articolul 26

Obligațiile implementatorilor de sisteme de IA cu grad ridicat de risc

- (1) Implementatorii sistemelor de IA cu grad ridicat de risc iau măsuri tehnice și organizatorice corespunzătoare pentru a oferi siguranța că utilizează astfel de sisteme în conformitate cu instrucțiunile de utilizare care însoțesc sistemele, în temeiul alineatelor (3) și (6).

- (2) Implementatorii încredințează supravegherea umană unor persoane fizice care au competența, formarea și autoritatea necesare, precum și sprijinul necesar.
- (3) Obligațiile de la alineatele (1) și (2) nu aduc atingere altor obligații ale implementatorilor în temeiul dreptului Uniunii sau al dreptului intern și nici libertății implementatorilor de a-și organiza propriile resurse și activități în scopul punerii în aplicare a măsurilor de supraveghere umană indicate de furnizor.
- (4) Fără a aduce atingere alineatelor (1) și (2), în măsura în care exercită controlul asupra datelor de intrare, implementatorul se asigură că datele de intrare sunt relevante și suficient de reprezentative în raport cu scopul preconizat al sistemului de IA cu grad ridicat de risc.
- (5) Implementatorii monitorizează funcționarea sistemului de IA cu grad ridicat de risc pe baza instrucțiunilor de utilizare și, atunci când este cazul, informează furnizorii în conformitate cu articolul 72. În cazul în care au motive să considere că utilizarea sistemului de IA cu grad ridicat de risc în conformitate cu instrucțiunile poate conduce la situația în care sistemul de IA respectiv prezintă un risc în sensul articolului 79 alineatul (1), implementatorii informează fără întârzieri nejustificate furnizorul sau distribuitorul și autoritatea relevantă de supraveghere a pieței și suspendă utilizarea sistemului respectiv. De asemenea, în cazul în care au identificat un incident grav, implementatorii informează imediat mai întâi furnizorul, și apoi importatorul sau distribuitorul și autoritățile relevante de supraveghere a pieței cu privire la incidentul respectiv. În cazul în care implementatorul nu poate comunica cu furnizorul, articolul 73 se aplică mutatis mutandis. Această obligație nu vizează datele operaționale sensibile ale implementatorilor sistemelor de IA care sunt autorități de aplicare a legii.

În cazul implementatorilor care sunt instituții financiare supuse unor cerințe privind guvernanta internă, măsurile sau procesele interne în temeiul dreptului Uniunii din domeniul serviciilor financiare, se consideră că obligația de monitorizare prevăzută la primul paragraf este îndeplinită prin respectarea normelor privind mecanismele, procesele și măsurile de guvernanta internă în temeiul dreptului relevant din domeniul serviciilor financiare.

- (6) Implementatorii sistemelor de IA cu grad ridicat de risc păstrează fișierele de jurnalizare generate automat de respectivele sisteme de IA cu grad ridicat de risc, în măsura în care aceste fișiere de jurnalizare se află sub controlul lor pentru o perioadă adecvată scopului preconizat al sistemului de IA cu grad ridicat de risc, de cel puțin șase luni, cu excepția cazului în care se prevede altfel în dreptul Uniunii sau în dreptul intern aplicabil, în special în dreptul Uniunii privind protecția datelor cu caracter personal.

Implementatorii care sunt instituții financiare supuse unor cerințe privind guvernanta internă, măsurile sau procesele interne în temeiul dreptului Uniunii din domeniul serviciilor financiare păstrează fișierele de jurnalizare ca parte a documentației păstrate în temeiul dreptului relevant al Uniunii din domeniul serviciilor financiare.

- (7) Înainte de a pune în funcțiune sau de a utiliza un sistem de IA cu grad ridicat de risc la locul de muncă, implementatorii care sunt angajatori informează reprezentanții lucrătorilor și lucrătorii afectați că vor fi implicați în utilizarea sistemului de IA cu grad ridicat de risc. Informațiile respective sunt furnizate, după caz, în conformitate cu normele și procedurile prevăzute în dreptul și practicile de la nivelul Uniunii și de la nivel național privind informarea lucrătorilor și a reprezentanților acestora.

- (8) Implementatorii sistemelor de IA cu grad ridicat de risc care sunt autorități publice sau instituții, organe, oficii sau agenții ale Uniunii respectă obligațiile de înregistrare menționate la articolul 49. În cazul în care constată că sistemul de IA cu grad ridicat de risc pe care intenționează să îl utilizeze nu a fost înregistrat în baza de date a UE menționată la articolul 71, implementatorii respectivi nu utilizează sistemul respectiv și informează furnizorul sau distribuitorul.
- (9) După caz, implementatorii de sisteme de IA cu grad ridicat de risc utilizează informațiile furnizate în temeiul articolului 13 din prezentul regulament pentru a-și respecta obligația de a efectua o evaluare a impactului asupra protecției datelor în temeiul articolului 35 din Regulamentul (UE) 2016/679 sau al articolului 27 din Directiva (UE) 2016/680.
- (10) Fără a aduce atingere Directivei (UE) 2016/680, în cadrul unei investigații pentru căutarea în mod specific a unei persoane suspectate sau condamnate de a fi comis o infracțiune, implementatorul unui sistem de IA cu grad ridicat de risc pentru identificarea biometrică la distanță ulterioară solicită o autorizație, *ex ante* sau fără întârzieri nejustificate și în termen de cel mult 48 de ore, din partea unei autorități judiciare sau a unei autorități administrative a cărei decizie are efect obligatoriu și face obiectul controlului jurisdicțional, pentru utilizarea sistemului respectiv, cu excepția cazului în care este utilizat pentru identificarea inițială a unui potențial suspect pe baza unor fapte obiective și verificabile legate direct de infracțiune. Fiecare utilizare se limitează la ceea ce este strict necesar pentru investigarea unei anumite infracțiuni.

În cazul în care autorizația solicitată în temeiul primului paragraf este respinsă, utilizarea sistemului de identificare biometrică la distanță ulterioară legat de autorizația solicitată respectivă se oprește cu efect imediat, iar datele cu caracter personal legate de utilizarea sistemului de IA cu grad ridicat de risc pentru care a fost solicitată autorizația se șterg.

În niciun caz, un astfel de sistem de IA cu grad ridicat de risc pentru identificarea biometrică la distanță ulterioară nu se utilizează într-un mod nedirecționat în scopul aplicării legii, dacă nu implică nicio legătură cu o infracțiune, cu o procedură penală, cu o amenințare reală și prezentă sau reală și previzibilă vizând o infracțiune sau căutarea unei anumite persoane dispărute. Se asigură faptul că autoritățile de aplicare a legii nu pot lua nicio decizie care produce un efect juridic negativ asupra unei persoane exclusiv pe baza rezultatelor unor astfel de sisteme de identificare biometrică la distanță ulterioară.

Prezentul alineat nu aduce atingere dispozițiilor de la articolul 9 din Regulamentul (UE) 2016/679 și de la articolul 10 din Directiva (UE) 2016/680 privind prelucrarea datelor biometrice.

Indiferent de scop sau de implementator, fiecare utilizare a acestor sisteme de IA cu grad ridicat de risc este documentată în dosarul relevant al poliției și este pusă la dispoziția autorității relevante de supraveghere a pieței și a autorității naționale pentru protecția datelor, la cerere, exceptând divulgarea datelor operaționale sensibile legate de aplicarea legii. Prezentul paragraf nu aduce atingere competențelor conferite autorităților de supraveghere de Directiva (UE) 2016/680.

Implementatorii prezintă autorităților relevante de supraveghere a pieței și autorităților naționale pentru protecția datelor rapoarte anuale cu privire la utilizarea sistemelor de identificare biometrică la distanță ulterioară, exceptând divulgarea datelor operaționale sensibile legate de aplicarea legii. Rapoartele pot fi agregate pentru a cuprinde mai multe implementări.

Statele membre pot introduce, în conformitate cu dreptul Uniunii, legi mai restrictive privind utilizarea sistemelor de identificare biometrică la distanță ulterioară.

- (11) Fără a afecta dispozițiile de la articolul 50 din prezentul regulament, implementatorii de sisteme de IA cu grad ridicat de risc menționate în anexa III, care iau decizii sau contribuie la luarea deciziilor referitoare la persoane fizice, informează persoanele fizice că fac obiectul utilizării sistemului de IA cu grad ridicat de risc. În cazul sistemelor de IA cu grad ridicat de risc utilizate în scopul aplicării legii, se aplică articolul 13 din Directiva (UE) 2016/680.
- (12) Implementatorii cooperează cu autoritățile competente relevante pentru orice acțiune întreprinsă de respectivele autorități în legătură cu sistemul de IA cu grad ridicat de risc pentru a pune în aplicare prezentul regulament.

Articolul 27

Evaluarea impactului sistemelor de IA cu grad ridicat de risc asupra drepturilor fundamentale

- (1) Înainte de a implementa un sistem de IA cu grad ridicat de risc, astfel cum este menționat la articolul 6 alineatul (2), cu excepția sistemelor de IA cu grad ridicat de risc destinate a fi utilizate în domeniul menționat la punctul 2 din anexa III, implementatorii care sunt organisme de drept public sau entități private care furnizează servicii publice și implementatorii de sisteme de IA cu grad ridicat de risc menționate la punctul 5 literele (b) și (c) din anexa III efectuează o evaluare a impactului asupra drepturilor fundamentale pe care îl poate produce utilizarea unor astfel de sisteme. În acest scop, implementatorii efectuează o evaluare care constă în:
- (a) o descriere a proceselor implementatorului în care sistemele de IA cu grad ridicat de risc urmează a fi utilizate în conformitate cu scopul lor preconizat;
 - (b) o descriere a perioadei de timp pentru care se intenționează utilizarea fiecărui sistem de IA cu grad ridicat de risc, precum și a frecvenței utilizării respective;

- (c) categoriile de persoane fizice și grupurile susceptibile a fi afectate de utilizarea sa în contextul specific;
 - (d) riscurile specifice de prejudicii susceptibile a avea un impact asupra categoriilor de persoane fizice sau a grupurilor de persoane identificate în temeiul literei (c) de la prezentul alineat, ținând seama de informațiile comunicate de furnizor în temeiul articolului 13;
 - (e) o descriere a punerii în aplicare a măsurilor de supraveghere umană, în conformitate cu instrucțiunile de utilizare;
 - (f) măsurile care trebuie să fie luate în cazul în care riscurile respective se materializează, inclusiv mecanismele de guvernanță internă și mecanismele de tratare a plângerilor.
- (2) Obligația prevăzută la alineatul (1) se aplică primei utilizări a sistemului de IA cu grad ridicat de risc. În cazuri similare, implementatorul poate să se bazeze pe evaluări ale impactului asupra drepturilor fundamentale efectuate anterior sau pe evaluări existente efectuate de furnizor. În cazul în care consideră că, în timpul utilizării sistemului de IA cu grad ridicat de risc, oricare dintre elementele enumerate la alineatul (1) s-a schimbat sau nu mai este actualizat, implementatorul ia măsurile necesare pentru a actualiza informațiile.
- (3) După efectuarea evaluării menționate la alineatul (1) de la prezentul articol, implementatorul notifică autorității de supraveghere a pieței rezultatele sale, transmițând modelul completat menționat la alineatul (5) de la prezentul articol ca parte a notificării. În cazul menționat la articolul 46 alineatul (1), implementatorii pot fi scutiți de această obligație de notificare.

- (4) În cazul în care oricare dintre obligațiile prevăzute la prezentul articol este deja respectată ca urmare a evaluării impactului asupra protecției datelor efectuate în temeiul articolului 35 din Regulamentul (UE) 2016/679 sau al articolului 27 din Directiva (UE) 2016/680, evaluarea impactului asupra drepturilor fundamentale menționată la alineatul (1) de la prezentul articol completează respectiva evaluare a impactului asupra protecției datelor.
- (5) Oficiul pentru IA elaborează un model de chestionar, inclusiv prin intermediul unui instrument automatizat, pentru a-i ajuta pe implementatori să își respecte obligațiile care le revin în temeiul prezentului articol într-un mod simplificat.

SECȚIUNEA 4

AUTORITĂȚILE DE NOTIFICARE ȘI ORGANISMELE NOTIFICATE

Articolul 28

Autoritățile de notificare

- (1) Fiecare stat membru desemnează sau instituie cel puțin o autoritate de notificare responsabilă cu instituirea și efectuarea procedurilor necesare pentru evaluarea, desemnarea și notificarea organismelor de evaluare a conformității și pentru monitorizarea acestora. Procedurile respective se elaborează în cooperare între autoritățile de notificare ale tuturor statelor membre.
- (2) Statele membre pot decide ca evaluarea și monitorizarea menționate la alineatul (1) să fie efectuate de un organism național de acreditare în sensul Regulamentului (CE) nr. 765/2008 și în conformitate cu acesta.

- (3) Autoritățile de notificare sunt instituite și organizate și funcționează astfel încât să nu apară niciun conflict de interese cu organismele de evaluare a conformității și să se protejeze obiectivitatea și imparțialitatea activităților lor.
- (4) Autoritățile de notificare sunt organizate astfel încât deciziile cu privire la notificarea organismelor de evaluare a conformității să fie luate de persoane competente, altele decât cele care au efectuat evaluarea organismelor respective.
- (5) Autoritățile de notificare nu oferă și nu prestează nici activități pe care le prestează organismele de evaluare a conformității și nici servicii de consultanță în condiții comerciale sau concurențiale.
- (6) Autoritățile de notificare garantează confidențialitatea informațiilor pe care le obțin, în conformitate cu articolul 78.
- (7) Autoritățile de notificare au la dispoziție un număr adecvat de membri competenți ai personalului în vederea îndeplinirii corespunzătoare a sarcinilor lor. Membrii competenți ai personalului dețin cunoștințele de specialitate necesare, după caz, pentru funcția pe care o îndeplinesc, în domenii precum tehnologiile informației, IA și drept, inclusiv supravegherea drepturilor fundamentale.

Articolul 29

Cererea de notificare a unui organism de evaluare a conformității

- (1) Organismele de evaluare a conformității depun o cerere de notificare la autoritatea de notificare a statului membru în care sunt stabilite.

- (2) Cererea de notificare este însoțită de o descriere a activităților de evaluare a conformității, a modulului sau modulelor de evaluare a conformității și a tipurilor de sisteme de IA pentru care organismul de evaluare a conformității se consideră a fi competent, precum și de un certificat de acreditare, în cazul în care există, eliberat de un organism național de acreditare care să ateste că organismul de evaluare a conformității satisface cerințele prevăzute la articolul 31.

Se adaugă orice document valabil referitor la desemnările existente ale organismului notificat solicitant în temeiul oricăror alte acte legislative de armonizare ale Uniunii.

- (3) În cazul în care un organism de evaluare a conformității nu poate prezenta un certificat de acreditare, acesta prezintă autorității de notificare toate documentele justificative necesare pentru verificarea, recunoașterea și monitorizarea periodică a conformității acestuia cu cerințele prevăzute la articolul 31.
- (4) În cazul organismelor notificate care sunt desemnate în temeiul oricăror alte acte legislative de armonizare ale Uniunii, toate documentele și certificatele legate de aceste desemnări pot fi utilizate pentru a sprijini procedura de desemnare a acestora în temeiul prezentului regulament, după caz. Organismul notificat actualizează documentația menționată la alineatele (2) și (3) de la prezentul articol ori de câte ori au loc modificări relevante, pentru a oferi autorității naționale responsabile de organismele notificate posibilitatea de a monitoriza și de a verifica respectarea continuă a tuturor cerințelor prevăzute la articolul 31.

Articolul 30
Procedura de notificare

- (1) Autoritățile de notificare pot notifica numai organismele de evaluare a conformității care îndeplinesc cerințele prevăzute la articolul 31.
- (2) Autoritățile de notificare înștiințează Comisia și celelalte state membre prin intermediul instrumentului de notificare electronică dezvoltat și administrat de Comisie cu privire la fiecare organism de evaluare a conformității menționat la alineatul (1).
- (3) Notificarea menționată la alineatul (2) de la prezentul articol include detalii complete privind activitățile de evaluare a conformității, modulul sau modulele de evaluare a conformității și tipurile de sisteme de IA în cauză, precum și atestarea relevantă a competenței. În cazul în care notificarea nu se bazează pe un certificat de acreditare menționat la articolul 29 alineatul (2), autoritatea de notificare prezintă Comisiei și celorlalte state membre documentele justificative care atestă competența organismului de evaluare a conformității și măsurile adoptate pentru a se asigura că organismul respectiv va fi monitorizat periodic și că va îndeplini în continuare cerințele prevăzute la articolul 31.
- (4) Organismul de evaluare a conformității în cauză poate exercita activitățile unui organism notificat numai în cazul în care nu există obiecții din partea Comisiei sau a celorlalte state membre, transmise în termen de două săptămâni de la o notificare din partea unei autorități de notificare, în cazul în care se include un certificat de acreditare menționat la articolul 29 alineatul (2), sau în termen de două luni de la o notificare din partea unei autorități de notificare, în cazul în care se includ documentele justificative menționate la articolul 29 alineatul (3).

- (5) În cazul în care se ridică obiecții, Comisia inițiază fără întârziere consultații cu statele membre relevante și cu organismul de evaluare a conformității. În lumina acestora, Comisia decide dacă autorizația este justificată. Comisia comunică decizia luată statului membru în cauză și organismului relevant de evaluare a conformității.

Articolul 31

Cerințe cu privire la organismele notificate

- (1) Un organism notificat este instituit în temeiul dreptului intern al unui stat membru și are personalitate juridică.
- (2) Organismele notificate îndeplinesc cerințele organizatorice, de management al calității, de resurse și în materie de procese care sunt necesare pentru îndeplinirea sarcinilor lor, precum și cerințele adecvate în materie de securitate cibernetică.
- (3) Structura organizațională, alocarea responsabilităților, liniile de raportare și funcționarea organismelor notificate asigură încrederea în performanța acestora și în rezultatele activităților de evaluare a conformității pe care le desfășoară organismele notificate.
- (4) Organismele notificate sunt independente de furnizorul unui sistem de IA cu grad ridicat de risc în legătură cu care efectuează activități de evaluare a conformității. Organismele notificate sunt, de asemenea, independente de orice alt operator care are un interes economic în legătură cu sistemele de IA cu grad ridicat de risc evaluate, precum și de orice concurent al furnizorului. Acest lucru nu împiedică utilizarea sistemelor de IA cu grad ridicat de risc evaluate care sunt necesare pentru operațiunile organismului de evaluare a conformității sau utilizarea sistemelor respective de IA cu grad ridicat de risc în scopuri personale.

- (5) Nici organismul de evaluare a conformității, personalul său de conducere de nivel superior, nici personalul responsabil cu îndeplinirea sarcinilor acestuia de evaluare a conformității nu sunt direct implicați în proiectarea, dezvoltarea, comercializarea sau utilizarea sistemelor de IA cu grad ridicat de risc și nici nu reprezintă părțile implicate în respectivele activități. Aceștia nu se implică în nicio activitate susceptibilă de a le afecta imparțialitatea sau integritatea în ceea ce privește activitățile de evaluare a conformității pentru care sunt notificați. Această dispoziție se aplică în special serviciilor de consultanță.
- (6) Organismele notificate sunt organizate și funcționează astfel încât să garanteze independența, obiectivitatea și imparțialitatea activităților lor. Organismele notificate documentează și pun în aplicare o structură și proceduri pentru garantarea imparțialității și pentru promovarea și punerea în practică a principiilor imparțialității în întreaga organizație, pentru tot personalul lor și pentru toate activitățile lor de evaluare.
- (7) Organismele notificate dispun de proceduri documentate care să asigure că personalul, comitetele, filialele, subcontractanții lor, precum și orice organism asociat sau membru al personalului organismelor externe respectă, în conformitate cu articolul 78, confidențialitatea informațiilor care le parvin în timpul derulării activităților de evaluare a conformității, cu excepția cazurilor în care divulgarea acestora este impusă prin lege. Personalul organismelor notificate este obligat să păstreze secretul profesional referitor la toate informațiile obținute în cursul îndeplinirii sarcinilor sale în temeiul prezentului regulament, excepție făcând relația cu autoritățile de notificare ale statului membru în care se desfășoară activitățile sale.

- (8) Organismele notificate dispun de proceduri pentru desfășurarea activităților, care să țină seama în mod corespunzător de dimensiunile unui furnizor, de sectorul în care acesta își desfășoară activitatea, de structura sa și de gradul de complexitate al sistemului de IA în cauză.
- (9) Organismele notificate încheie o asigurare de răspundere civilă adecvată pentru activitățile lor de evaluare a conformității, cu excepția cazului în care răspunderea este asumată de statul membru pe teritoriul căruia sunt stabilite, în conformitate cu dreptul intern, sau în care însuși statul membru respectiv este direct responsabil pentru evaluarea conformității.
- (10) Organismele notificate sunt capabile să își îndeplinească toate sarcinile în temeiul prezentului regulament cu cel mai înalt grad de integritate profesională și cu competența necesară în domeniul specific, indiferent dacă sarcinile respective sunt realizate de organisme notificate înseși sau în numele și pe răspunderea acestora.
- (11) Organismele notificate dispun de suficiente competențe interne pentru a putea evalua în mod efectiv sarcinile îndeplinite de părți externe în numele lor. Organismul notificat dispune în permanență de suficient personal administrativ, tehnic, juridic și științific care deține experiență și cunoștințe în ceea ce privește tipurile relevante de sisteme de IA, de date și de calculul datelor, precum și în ceea ce privește cerințele prevăzute în secțiunea 2.
- (12) Organismele notificate participă la activitățile de coordonare menționate la articolul 38. De asemenea, acestea participă direct sau sunt reprezentate în cadrul organizațiilor de standardizare europene sau se asigură că sunt la curent cu situația referitoare la standardele relevante.

Articolul 32

Prezumția de conformitate cu cerințele referitoare la organismele notificate

În cazul în care un organism de evaluare a conformității își demonstrează conformitatea cu criteriile prevăzute în standardele armonizate relevante sau în părți din acestea, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*, se consideră că acesta este în conformitate cu cerințele prevăzute la articolul 31, în măsura în care standardele armonizate aplicabile vizează aceste cerințe.

Articolul 33

Filiale ale organismelor notificate și subcontractare

- (1) În cazul în care un organism notificat subcontractează anumite sarcini legate de evaluarea conformității sau recurge la o filială, acesta se asigură că subcontractantul sau filiala îndeplinește cerințele stabilite la articolul 31 și informează autoritatea de notificare în acest sens.
- (2) Organismele notificate preiau întreaga responsabilitate pentru sarcinile îndeplinite de orice subcontractant sau filială.
- (3) Activitățile pot fi subcontractate sau îndeplinite de o filială doar cu acordul furnizorului. Organismele notificate pun la dispoziția publicului o listă a filialelor acestora.
- (4) Documentele relevante privind evaluarea calificărilor subcontractantului sau ale filialei și activitatea desfășurată de aceștia în temeiul prezentului regulament sunt puse la dispoziția autorității de notificare pentru o perioadă de cinci ani de la data încetării subcontractării.

Articolul 34

Obligații operaționale ale organismelor notificate

- (1) Organismele notificate verifică conformitatea sistemelor de IA cu grad ridicat de risc în conformitate cu procedurile de evaluare a conformității prevăzute la articolul 43.
- (2) Organismele notificate evită sarcinile inutile pentru furnizori atunci când aceștia își desfășoară activitățile și țin seama în mod corespunzător de dimensiunile furnizorilor, de sectorul în care aceștia își desfășoară activitatea, de structura acestora și de gradul de complexitate al sistemului de IA cu grad ridicat de risc în cauză, în special în vederea reducerii la minimum a sarcinilor administrative și a costurilor de asigurare a conformității pentru microîntreprinderi și întreprinderile mici în sensul Recomandării 2003/361/CE. Organismul notificat respectă totuși gradul de precizie și nivelul de protecție impuse pentru conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prezentului regulament..
- (3) Organismele notificate pun la dispoziția autorității de notificare menționate la articolul 28 și transmit la cerere toată documentația relevantă, inclusiv documentația furnizorilor, pentru a îi permite acestei autorități să își desfășoare activitățile de evaluare, desemnare, notificare și monitorizare și pentru a facilita evaluarea descrisă în prezenta secțiune.

Articolul 35

Numerele de identificare și listele organismelor notificate

- (1) Comisia atribuie un număr unic de identificare fiecărui organism notificat, chiar și în cazul în care un organism este notificat în temeiul mai multor acte ale Uniunii.

- (2) Comisia pune la dispoziția publicului lista organismelor notificate în temeiul prezentului regulament, incluzând numerele de identificare ale acestora și activitățile pentru care au fost notificate. Comisia se asigură că lista este actualizată.

Articolul 36

Modificări ale notificărilor

- (1) Autoritatea de notificare înștiințează Comisia și celelalte state membre cu privire la orice modificare relevantă adusă notificării unui organism notificat prin intermediul instrumentului de notificare electronică menționat la articolul 30 alineatul (2).
- (2) Procedurile prevăzute la articolele 29 și 30 se aplică extinderilor domeniului de aplicare al notificării.

În ceea ce privește modificările aduse notificării, altele decât extinderile domeniului său de aplicare, se aplică procedurile prevăzute la alineatele (3)-(9).

- (3) În cazul în care un organism notificat decide să își înceteze activitățile de evaluare a conformității, acesta informează autoritatea de notificare și furnizorii vizați cât mai curând posibil și, în cazul unei încetări planificate, cu cel puțin un an înainte de încetarea activităților. Certificatele organismului notificat pot rămâne valabile pentru o perioadă de nouă luni de la încetarea activității organismului notificat, cu condiția ca un alt organism notificat să fi confirmat în scris că își va asuma responsabilitățile pentru sistemele de IA cu grad ridicat de risc care fac obiectul respectivelor certificate. Acest din urmă organism notificat efectuează o evaluare completă a sistemelor de IA cu grad ridicat de risc în cauză până la finalul respectivei perioade de nouă luni, înainte de emiterea de noi certificate pentru aceste sisteme. În cazul în care organismul notificat și-a încetat activitatea, autoritatea de notificare retrage desemnarea.

- (4) În cazul în care o autoritate de notificare are motive suficiente să considere că un organism notificat nu mai îndeplinește cerințele prevăzute la articolul 31 sau că acesta nu își îndeplinește obligațiile, autoritatea de notificare respectivă investighează fără întârziere chestiunea, cu cea mai mare diligență. În acest context, aceasta informează organismul notificat în cauză cu privire la obiecțiile ridicate și îi oferă posibilitatea de a-și face cunoscute punctele de vedere. În cazul în care ajunge la concluzia că organismul notificat nu mai îndeplinește cerințele prevăzute la articolul 31 sau că nu își îndeplinește obligațiile, autoritatea de notificare restricționează, suspendă sau retrage desemnarea, după caz, în funcție de gravitatea încălcării cerințelor sau a neîndeplinirii obligațiilor. Autoritatea de notificare informează de îndată Comisia și celelalte state membre în consecință.
- (5) În cazul în care desemnarea sa a fost suspendată, restricționată sau retrasă integral sau parțial, organismul notificat informează furnizorii în cauză în termen de 10 zile.
- (6) În caz de restricționare, suspendare sau retragere a unei desemnări, autoritatea de notificare ia măsurile necesare pentru a se asigura că dosarele organismului notificat în cauză sunt păstrate și le pun la dispoziția autorităților de notificare din alte state membre și a autorităților de supravegherea pieței, la cererea acestora.
- (7) În caz de restricționare, suspendare sau retragere a unei desemnări, autoritatea de notificare:
- (a) evaluează impactul asupra certificatelor eliberate de organismul notificat;
 - (b) prezintă Comisiei și celorlalte state membre un raport conținând constatările sale în termen de trei luni de la data la care a notificat modificările aduse desemnării;

- (c) solicită organismului notificat să suspende sau să retragă, într-un interval rezonabil de timp stabilit de către autoritate, orice certificat care a fost eliberat în mod necorespunzător, pentru a asigura menținerea conformității sistemelor de IA cu grad ridicat de risc de pe piață;
 - (d) informează Comisia și statele membre cu privire la certificatele pentru care a solicitat suspendarea sau retragerea;
 - (e) furnizează autorităților naționale competente din statul membru în care furnizorul își are sediul social toate informațiile relevante cu privire la certificatele pentru care a solicitat suspendarea sau retragerea; autoritățile respective iau măsurile corespunzătoare, acolo unde este necesar, pentru evitarea unui risc potențial pentru sănătate, siguranță sau drepturile fundamentale.
- (8) Cu excepția certificatelor eliberate în mod necorespunzător și în cazul în care o desemnare a fost suspendată sau restricționată, certificatele rămân valabile în una dintre următoarele circumstanțe:
- (a) autoritatea de notificare a confirmat, în termen de o lună de la suspendare sau restricționare, că nu există niciun risc pentru sănătate, siguranță sau drepturile fundamentale în legătură cu certificatele afectate de suspendare sau de restricționare și a prezentat un calendar pentru acțiunile de remediere a suspendării sau a restricționării; sau

- (b) autoritatea de notificare a confirmat că, pe durata suspendării sau restricționării nu se va emite, modifica sau emite din nou niciun certificat relevant pentru suspendare și declară dacă organismul notificat are capacitatea de a continua să monitorizeze și să rămână responsabil de certificatele existente pe care le-a emis pe perioada suspendării sau a restricționării; în cazul în care autoritatea de notificare stabilește că organismul notificat nu are capacitatea de a gestiona certificatele existente pe care le-a emis, furnizorul sistemului care face obiectul certificatului confirmă în scris autorităților naționale competente ale statului membru în care își are sediul social, în termen de trei luni de la suspendare sau restricționare, că un alt organism notificat calificat își asumă temporar funcțiile organismului notificat de a monitoriza și de a rămâne responsabil de certificate pe perioada suspendării sau a restricționării.
- (9) Cu excepția certificatelor eliberate în mod necorespunzător și, în cazul în care desemnarea a fost retrasă, certificatele rămân valabile pe o perioadă de nouă luni în următoarele circumstanțe:
- (a) autoritatea națională competentă din statul membru în care furnizorul sistemului de IA cu grad ridicat de risc care face obiectul certificatului își are sediul social a confirmat că nu există niciun risc pentru sănătate, siguranță sau drepturile fundamentale asociat sistemelor de IA cu grad ridicat de risc în cauză; și
- (b) un alt organism notificat a confirmat în scris că își va asuma responsabilitatea imediat pentru respectivele sisteme de IA și își încheie evaluarea în termen de 12 luni de la retragerea desemnării.

În situația menționată la primul paragraf, autoritatea națională competentă din statul membru în care își are sediul social furnizorul sistemului care face obiectul certificatului poate prelungi valabilitatea provizorie a certificatelor cu perioade suplimentare de trei luni, care nu depășesc 12 luni în total.

Autoritatea națională competentă sau organismul notificat care își asumă funcțiile organismului notificat afectat de modificarea desemnării informează imediat în acest sens Comisia, celelalte state membre și celelalte organisme notificate.

Articolul 37

Contestarea competenței organismelor notificate

- (1) Dacă este necesar, Comisia investighează toate cazurile în care există motive de îndoială cu privire la competența unui organism notificat sau la îndeplinirea în continuare de către un organism notificat a cerințelor prevăzute la articolul 31 și a responsabilităților sale aplicabile.
- (2) Autoritatea de notificare furnizează Comisiei, la cerere, toate informațiile relevante referitoare la notificarea sau menținerea competenței organismului notificat în cauză.
- (3) Comisia se asigură că toate informațiile sensibile obținute în cursul investigațiilor sale în temeiul prezentului articol sunt tratate în mod confidențial în conformitate cu articolul 78.

- (4) În cazul în care constată că un organism notificat nu îndeplinește sau nu mai îndeplinește cerințele pentru a fi notificat, Comisia informează statul membru notificator în consecință și îi solicită acestuia să ia măsurile corective necesare, inclusiv suspendarea sau retragerea notificării, dacă este necesar. În cazul în care statul membru nu ia măsurile corective necesare, Comisia poate, prin intermediul unui act de punere în aplicare, să suspende, să restricționeze sau să retragă desemnarea. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Articolul 38

Coordonarea organismelor notificate

- (1) Comisia se asigură că, în ceea ce privește sistemele de IA cu grad ridicat de risc, se instituie și se realizează în mod adecvat o coordonare și o cooperare corespunzătoare între organisme notificate care desfășoară activități în ceea ce privește procedurile de evaluare a conformității în temeiul prezentului regulament, sub forma unui grup sectorial al organismelor notificate.
- (2) Fiecare autoritate de notificare se asigură că organisme notificate de aceasta participă la activitatea unui grup menționat la alineatul (1), în mod direct sau prin intermediul unor reprezentanți desemnați.
- (3) Comisia se ocupă de organizarea unor schimburi de cunoștințe și bune practici între autoritățile de notificare.

Articolul 39

Organisme de evaluare a conformității din țări terțe

Organismele de evaluare a conformității instituite în temeiul legislației unei țări terțe cu care Uniunea a încheiat un acord pot fi autorizate să desfășoare activitățile organismelor notificate în temeiul prezentului regulament, cu condiția ca aceste organisme să îndeplinească cerințele prevăzute la articolul 31 sau să asigure un nivel de conformitate echivalent.

SECȚIUNEA 5

STANDARDE, EVALUAREA CONFORMITĂȚII, CERTIFICATE, ÎNREGISTRARE

Articolul 40

Standarde armonizate și documente de standardizare

- (1) Sistemele de IA cu grad ridicat de risc sau modelele de IA de uz general care sunt în conformitate cu standardele armonizate sau cu o parte a acestora, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene* în conformitate cu Regulamentul (UE) nr. 1025/2012, sunt considerate a fi în conformitate cu cerințele stabilite în secțiunea 2 din prezentul capitol sau, după caz, cu obligațiile prevăzute în capitolul V secțiunile 2 și 3 din prezentul regulament, în măsura în care standardele respective vizează cerințele sau obligațiile respective.

- (2) În conformitate cu articolul 10 din Regulamentul (UE) nr. 1025/2012, Comisia emite, fără întârzieri nejustificate, solicitări de standardizare care vizează toate cerințele prevăzute în secțiunea 2 din prezentul capitol și, după caz, solicitări de standardizare care vizează obligațiile prevăzute în capitolul V secțiunile 2 și 3 din prezentul regulament. De asemenea, în cadrul solicitărilor de standardizare se cere furnizarea de documente privind procesele de raportare și documentare pentru a îmbunătăți performanța în materie de resurse a sistemelor de IA, cum ar fi reducerea consumului de energie și de alte resurse pentru sistemul de IA cu grad ridicat de risc pe parcursul ciclului său de viață, precum și privind dezvoltarea eficientă din punct de vedere energetic a modelelor de IA de uz general. Atunci când elaborează o solicitare de standardizare, Comisia consultă Consiliul IA și părțile interesate relevante, inclusiv forumul consultativ.

Atunci când adresează o solicitare de standardizare organizațiilor de standardizare europene, Comisia precizează că standardele trebuie să fie clare și coerente inclusiv cu standardele elaborate în diferitele sectoare pentru produsele care fac obiectul legislației existente de armonizare a Uniunii care figurează în anexa I, având drept scop să asigure faptul că sistemele de IA cu grad ridicat de risc sau modelele de IA de uz general introduse pe piață sau puse în funcțiune în Uniune îndeplinesc cerințele sau obligațiile relevante prevăzute în prezentul regulament.

Comisia solicită organizațiilor de standardizare europene să furnizeze dovezi ale tuturor eforturilor depuse pentru a îndeplini obiectivele menționate la primul și al doilea paragraf de la prezentul alineat, în conformitate cu articolul 24 din Regulamentul (UE) nr. 1025/2012.

- (3) Participanții la procesul de standardizare urmăresc să promoveze investițiile și inovarea în IA, inclusiv prin sporirea securității juridice, precum și competitivitatea și creșterea pieței Uniunii, să contribuie la consolidarea cooperării la nivel mondial în materie de standardizare, ținând seama de standardele internaționale existente în domeniul IA care sunt în concordanță cu valorile, drepturile fundamentale și interesele Uniunii, și să consolideze guvernanta multipartită, asigurând o reprezentare echilibrată a intereselor și participarea efectivă a tuturor părților interesate relevante, în conformitate cu articolele 5, 6 și 7 din Regulamentul (UE) nr. 1025/2012.

Articolul 41

Specificații comune

- (1) Comisia poate să adopte acte de punere în aplicare de stabilire a specificațiilor comune pentru cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, pentru obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, în cazul în care sunt îndeplinite următoarele condiții:
- (a) Comisia a solicitat, în temeiul articolului 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012, uneia sau mai multor organizații de standardizare europene să elaboreze un standard armonizat pentru cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, pentru obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, și:
- (i) solicitarea nu a fost acceptată de niciuna dintre organizațiile de standardizare europene; sau

- (ii) nu sunt prezentate standarde armonizate care să răspundă solicitării respective în termenul stabilit în conformitate cu articolul 10 alineatul (1) din Regulamentul (UE) nr. 1025/2012; sau
 - (iii) standardele armonizate relevante nu abordează suficient preocupările legate de drepturile fundamentale; sau
 - (iv) standardele armonizate nu sunt conforme cu solicitarea; și
- (b) nicio referință la standardele armonizate care vizează cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, nu a fost publicată în *Jurnalul Oficial al Uniunii Europene* în conformitate cu Regulamentul (UE) nr. 1025/2012, și nu se preconizează publicarea niciunei astfel de referințe într-un termen rezonabil.

La redactarea specificațiilor comune, Comisia consultă forumul consultativ menționat la articolul 67.

Actele de punere în aplicare menționate la primul paragraf de la prezentul alineat se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

- (2) Înainte de a pregăti un proiect de act de punere în aplicare, Comisia informează comitetul menționat la articolul 22 din Regulamentul (UE) nr. 1025/2012 că, în opinia sa, sunt îndeplinite condițiile de la alineatul (1).

- (3) Sistemele de IA cu grad ridicat de risc sau modelele de IA de uz general care sunt în conformitate cu specificațiile comune menționate la alineatul (1) sau cu părți ale acestora sunt considerate a fi în conformitate cu cerințele prevăzute în secțiunea 2 din prezentul capitol sau, după caz, a respecta obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, în măsura în care respectivele specificații comune vizează cerințele sau obligațiile respective.
- (4) În cazul în care un standard armonizat este adoptat de o organizație de standardizare europeană și este propus Comisiei pentru ca referința sa să fie publicată în *Jurnalul Oficial al Uniunii Europene*, Comisia evaluează standardul armonizat în conformitate cu Regulamentul (UE) nr. 1025/2012. Atunci când referința unui standard armonizat este publicată în *Jurnalul Oficial al Uniunii Europene*, Comisia abrogă actele de punere în aplicare menționate la alineatul (1) sau acele părți ale lor care vizează aceleași cerințe menționate la secțiunea 2 din prezentul capitol sau, după caz, aceleași obligații prevăzute în secțiunile 2 și 3 din capitolul V.
- (5) În cazul în care furnizorii de sisteme de IA cu grad ridicat de risc sau de modele de IA de uz general nu respectă specificațiile comune menționate la alineatul (1), aceștia trebuie să dovedească în mod corespunzător faptul că au adoptat soluții tehnice care îndeplinesc cerințele menționate în secțiunea 2 din prezentul capitol sau, după caz, care respectă obligațiile prevăzute în secțiunile 2 și 3 din capitolul V la un nivel cel puțin echivalent cu acestea.

- (6) În cazul în care un stat membru consideră că o specificație comună nu îndeplinește în totalitate cerințele prevăzute în secțiunea 2 sau, după caz, nu respectă în totalitate obligațiile prevăzute în secțiunile 2 și 3 din capitolul V, acesta informează Comisia în acest sens, furnizând o explicație detaliată. Comisia evaluează informațiile respective și, dacă este cazul, modifică actul de punere în aplicare prin care se stabilește specificația comună în cauză.

Articolul 42

Prezumția de conformitate cu anumite cerințe

- (1) Sistemele de IA cu grad ridicat de risc care au fost antrenate și testate pe baza datelor care reflectă mediul geografic, comportamental, contextual sau funcțional specific în care sunt destinate să fie utilizate sunt considerate a respecta cerințele relevante prevăzute la articolul 10 alineatul (4).
- (2) Sistemele de IA cu grad ridicat de risc care au fost certificate sau pentru care a fost emisă o declarație de conformitate în cadrul unui sistem de securitate cibernetică în temeiul Regulamentului (UE) 2019/881, iar referințele aferente au fost publicate în *Jurnalul Oficial al Uniunii Europene*, sunt considerate a respecta cerințele de securitate cibernetică prevăzute la articolul 15 din prezentul regulament în măsura în care certificatul de securitate cibernetică sau declarația de conformitate sau părți ale acestora vizează cerințele respective.

Articolul 43
Evaluarea conformității

- (1) Pentru sistemele de IA cu grad ridicat de risc enumerate la punctul 1 din anexa III, în cazul în care, pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, furnizorul a aplicat standardele armonizate menționate la articolul 40 sau, după caz, specificațiile comune menționate la articolul 41, furnizorul optează pentru una dintre următoarele proceduri de evaluare a conformității:
- (a) controlul intern, menționat în anexa VI; sau
 - (b) evaluarea sistemului de management al calității și examinarea documentației tehnice, cu implicarea unui organism notificat, menționată în anexa VII.

Pentru a demonstra conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, furnizorul urmează procedura de evaluare a conformității prevăzută în anexa VII în următoarele cazuri:

- (a) standardele armonizate menționate la articolul 40 nu există, iar specificațiile comune menționate la articolul 41 nu sunt disponibile;
- (b) furnizorul nu a aplicat sau a aplicat doar o parte din standardul armonizat;
- (c) specificațiile comune menționate la litera (a) există, dar furnizorul nu le-a aplicat;

- (d) unul sau mai multe dintre standardele armonizate menționate la litera (a) au fost publicate cu o restricție și numai în partea standardului care a fost restricționată.

În sensul procedurii de evaluare a conformității menționate în anexa VII, furnizorul poate alege oricare dintre organismele notificate. Cu toate acestea, în cazul în care sistemul de IA cu grad ridicat de risc este destinat să fie pus în funcțiune de către autoritățile de aplicare a legii, de imigrație sau de azil, sau de către instituțiile, organele, oficiile sau agențiile Uniunii, autoritatea de supraveghere a pieței menționată la articolul 74 alineatul (8) sau (9), după caz, acționează ca organism notificat.

- (2) În cazul sistemelor de IA cu grad ridicat de risc menționate la punctele 2-8 din anexa III, furnizorii urmează procedura de evaluare a conformității bazată pe controlul intern, astfel cum se menționează în anexa VI, care nu prevede implicarea unui organism notificat.
- (3) În cazul sistemelor de IA cu grad ridicat de risc cărora li se aplică actele juridice de armonizare ale Uniunii care figurează în anexa I secțiunea A, furnizorul urmează procedura de evaluare a conformității relevantă, astfel cum se prevede în actele juridice respective. Cerințele prevăzute în secțiunea 2 din prezentul capitol se aplică acestor sisteme de IA cu grad ridicat de risc și fac parte din evaluarea respectivă. Se aplică, de asemenea, punctele 4.3, 4.4, 4.5 și punctul 4.6 al cincilea paragraf din anexa VII.

În scopul evaluării respective, organismele notificate care au fost notificate în temeiul respectivelor acte juridice au dreptul de a controla conformitatea sistemelor de IA cu grad ridicat de risc cu cerințele prevăzute în secțiunea 2, cu condiția ca respectarea de către organismele notificate respective a cerințelor prevăzute la articolul 31 alineatele (4), (10) și (11) să fi fost evaluată în contextul procedurii de notificare în temeiul respectivelor acte juridice.

În cazul în care actele juridice care figurează în anexa I secțiunea A permit fabricantului produsului să renunțe la evaluarea conformității efectuată de o parte terță, cu condiția ca fabricantul respectiv să fi aplicat toate standardele armonizate care vizează toate cerințele relevante, fabricantul respectiv poate recurge la această opțiune numai dacă a aplicat, de asemenea, standardele armonizate sau, după caz, specificațiile comune menționate la articolul 41, care vizează toate cerințele prevăzute în secțiunea 2 din prezentul capitol.

- (4) Sistemele de IA cu grad ridicat de risc care au făcut deja obiectul unei proceduri de evaluare a conformității sunt supuse la o nouă procedură de evaluare a conformității în cazul unei modificări substanțiale, indiferent dacă sistemul modificat este destinat să fie distribuit mai departe sau dacă implementatorul actual continuă să utilizeze sistemul modificat.

În cazul sistemelor de IA cu grad ridicat de risc care continuă să învețe după ce au fost introduse pe piață sau puse în funcțiune, modificările aduse sistemului de IA cu grad ridicat de risc și performanței acestuia care au fost predeterminate de către furnizor la momentul evaluării inițiale a conformității și care fac parte din informațiile conținute în documentația tehnică menționată la punctul 2 litera (f) din anexa IV nu constituie o modificare substanțială.

- (5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 în scopul modificării anexelor VI și VII prin actualizarea acestora având în vedere progresele tehnice.

- (6) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica alineatele (1) și (2) de la prezentul articol cu scopul de a supune sistemele de IA cu grad ridicat de risc menționate la punctele 2-8 din anexa III procedurii de evaluare a conformității menționate în anexa VII sau unor părți ale acesteia. Comisia adoptă astfel de acte delegate ținând seama de eficacitatea procedurii de evaluare a conformității bazate pe controlul intern menționate în anexa VI în ceea ce privește prevenirea sau reducerea la minimum a riscurilor pentru sănătate, siguranță și protecția drepturilor fundamentale pe care le prezintă astfel de sisteme, precum și de disponibilitatea capacităților și a resurselor adecvate în cadrul organismelor notificate.

Articolul 44

Certificate

- (1) Certificatele eliberate de organismele notificate în conformitate cu anexa VII sunt redactate într-o limbă care poate fi ușor înțeleasă de autoritățile relevante din statul membru în care este stabilit organismul notificat.
- (2) Certificatele sunt valabile pe perioada pe care o indică, care nu depășește cinci ani pentru sistemele de IA vizate de anexa I și patru ani pentru sistemele de IA vizate de anexa III. La solicitarea furnizorului, valabilitatea unui certificat poate fi prelungită pentru perioade suplimentare, fiecare dintre acestea nedepășind cinci ani pentru sistemele de IA vizate de anexa I și patru ani pentru sistemele de IA vizate de anexa III, pe baza unei reevaluări în conformitate cu procedurile aplicabile de evaluare a conformității. Orice supliment la un certificat rămâne valabil, cu condiția ca certificatul pe care îl completează să fie valabil.

- (3) În cazul în care un organism notificat constată că un sistem de IA nu mai îndeplinește cerințele prevăzute în secțiunea 2, acesta, ținând seama de principiul proporționalității, suspendă sau retrage certificatul eliberat sau impune restricții asupra acestuia, cu excepția cazului în care îndeplinirea cerințelor respective este asigurată prin măsuri corective adecvate întreprinse de furnizorul sistemului într-un termen adecvat stabilit de organismul notificat. Organismul notificat comunică motivele deciziei sale.

Se pune la dispoziție o cale de atac împotriva deciziilor organismelor notificate, inclusiv privind certificatele de conformitate eliberate.

Articolul 45

Obligații de informare care revin organismelor notificate

- (1) Organismele notificate informează autoritatea de notificare în legătură cu:
- (a) orice certificate de evaluare a documentației tehnice ale Uniunii, orice suplimente la certificatele respective și orice aprobări ale sistemului de management al calității eliberate în conformitate cu cerințele din anexa VII;
 - (b) orice refuz, restricție, suspendare sau retragere a unui certificat de evaluare a documentației tehnice al Uniunii sau a unei aprobări a unui sistem de management al calității eliberată în conformitate cu cerințele din anexa VII;
 - (c) orice circumstanță care afectează domeniul de aplicare sau condițiile notificării;

- (d) orice cerere de informații pe care au primit-o de la autoritățile de supraveghere a pieței cu privire la activitățile de evaluare a conformității;
 - (e) la cerere, activitățile de evaluare a conformității realizate în limita domeniului de aplicare al notificării lor și orice altă activitate realizată, inclusiv activități transfrontaliere și subcontractare.
- (2) Fiecare organism notificat informează celelalte organisme notificate cu privire la:
- (a) aprobări ale sistemelor de management al calității pe care le-a refuzat, suspendat sau retras și, la cerere, aprobări ale sistemelor de management al calității pe care le-a eliberat;
 - (b) certificatele de evaluare a documentației tehnice ale Uniunii sau orice suplimente la acestea, pe care le-a refuzat, retras, suspendat sau restricționat în alt mod și, la cerere, certificatele și/sau suplimentele la acestea pe care le-a eliberat.
- (3) Fiecare organism notificat furnizează celorlalte organisme notificate care îndeplinesc activități similare de evaluare a conformității, care vizează aceleași tipuri de sisteme de IA, informații relevante privind aspecte legate de rezultatele negative ale evaluărilor conformității și, la cerere, de rezultatele pozitive ale evaluărilor conformității.
- (4) Organismele notificate păstrează confidențialitatea informațiilor pe care le obțin, în conformitate cu articolul 78.

Articolul 46

Derogare de la procedura de evaluare a conformității

- (1) Prin derogare de la articolul 43 și pe baza unei cereri justificate în mod corespunzător, orice autoritate de supraveghere a pieței poate autoriza introducerea pe piață sau punerea în funcțiune a anumitor sisteme de IA cu grad ridicat de risc pe teritoriul statului membru în cauză, din motive excepționale de siguranță publică sau de protecție a vieții și sănătății persoanelor, de protecție a mediului sau de protecție a activelor industriale și de infrastructură esențiale. Autorizația respectivă se acordă pentru o perioadă limitată, cât timp procedurile necesare de evaluare a conformității sunt în desfășurare, ținând seama de motivele excepționale care justifică derogarea. Finalizarea procedurilor respective se efectuează fără întârzieri nejustificate.
- (2) Într-o situație de urgență justificată în mod corespunzător din motive excepționale de securitate publică sau în cazul unei amenințări specifice, substanțiale și iminente la adresa vieții sau a siguranței fizice a persoanelor fizice, autoritățile de aplicare a legii sau autoritățile de protecție civilă pot pune în funcțiune un anumit sistem de IA cu grad ridicat de risc fără autorizația menționată la alineatul (1), cu condiția ca o astfel de autorizație să fie solicitată în timpul utilizării sau după aceasta, fără întârzieri nejustificate. În cazul în care autorizația menționată la alineatul (1) este refuzată, utilizarea sistemului de IA cu grad ridicat de risc este oprită cu efect imediat și toate rezultatele și produsele obținute în cadrul unei astfel de utilizări sunt înlăturate imediat.

- (3) Autorizația menționată la alineatul (1) se eliberează numai în cazul în care autoritatea de supraveghere a pieței concluzionează că sistemul de IA cu grad ridicat de risc respectă cerințele din secțiunea 2. Autoritatea de supraveghere a pieței informează Comisia și celelalte state membre cu privire la orice autorizație eliberată în temeiul alineatelor (1) și (2). Această obligație nu vizează datele operaționale sensibile legate de activitățile autorităților de aplicare a legii.
- (4) În cazul în care, în termen de 15 zile calendaristice de la primirea informațiilor menționate la alineatul (3), niciun stat membru și nici Comisia nu ridică obiecții cu privire la o autorizație eliberată de o autoritate de supraveghere a pieței dintr-un stat membru în conformitate cu alineatul (1), autorizația respectivă este considerată justificată.
- (5) În cazul în care, în termen de 15 zile calendaristice de la primirea notificării menționate la alineatul (3), sunt ridicate obiecții de către un stat membru împotriva unei autorizații eliberate de o autoritate de supraveghere a pieței dintr-un alt stat membru sau în cazul în care Comisia consideră că autorizația este contrară dreptului Uniunii sau că concluzia statelor membre cu privire la conformitatea sistemului, astfel cum se menționează la alineatul (3), este nefondată, Comisia inițiază fără întârziere consultări cu statul membru relevant. Operatorii în cauză sunt consultați și au posibilitatea de a-și prezenta punctele de vedere. În considerarea acestora, Comisia decide dacă autorizația este justificată. Comisia comunică decizia sa statelor membre în cauză și operatorilor relevanți.
- (6) În cazul în care Comisia consideră că autorizația este nejustificată, aceasta este retrasă de către autoritatea de supraveghere a pieței din statul membru în cauză.

- (7) Pentru sistemele de IA cu grad ridicat de risc legate de produsele care fac obiectul actelor legislative de armonizare ale Uniunii menționate în anexa I secțiunea A, se aplică numai derogări de la procedurile de evaluare a conformității stabilite în respectivele acte legislative de armonizare ale Uniunii.

Articolul 47

Declarația de conformitate UE

- (1) Furnizorul întocmește o declarație de conformitate UE elaborată într-un format prelucrabil automat, cu semnătură fizică sau electronică pentru fiecare sistem de IA cu grad ridicat de risc și o pune la dispoziția autorităților naționale competente pe o perioadă de 10 ani după introducerea pe piață sau punerea în funcțiune a sistemului de IA cu grad ridicat de risc. Declarația de conformitate UE identifică sistemul de IA cu grad ridicat de risc pentru care a fost întocmită. O copie a declarației de conformitate UE este transmisă autorităților naționale competente relevante, la cerere.
- (2) Declarația de conformitate UE precizează că sistemul de IA cu grad ridicat de risc în cauză îndeplinește cerințele prevăzute în secțiunea 2. Declarația de conformitate UE conține informațiile prevăzute în anexa V și se traduce într-o limbă care poate fi ușor înțeleasă de autoritățile naționale competente din statele membre în care se introduce pe piață sau se pune la dispoziție sistemul de IA cu grad ridicat de risc.

- (3) În cazul în care sistemele de IA cu grad ridicat de risc fac obiectul altor acte legislative de armonizare ale Uniunii care necesită, de asemenea, o declarație de conformitate UE, se redactează o singură declarație de conformitate UE în legătură cu toate actele legislative ale Uniunii aplicabile sistemului de IA cu grad ridicat de risc. Declarația conține toate informațiile necesare pentru identificarea actelor legislative de armonizare ale Uniunii cu care are legătură declarația.
- (4) Prin redactarea declarației de conformitate UE, furnizorul își asumă responsabilitatea pentru conformitatea cu cerințele prevăzute în secțiunea 2. Furnizorul actualizează în permanență declarația de conformitate UE, după caz.
- (5) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa V prin actualizarea conținutului declarației de conformitate UE prevăzute în anexa menționată, pentru a introduce elemente care devin necesare având în vedere progresele tehnice.

Articolul 48

Marcajul CE

- (1) Marcajul CE face obiectul principiilor generale prevăzute la articolul 30 din Regulamentul (CE) nr. 765/2008.
- (2) În cazul sistemelor de IA cu grad ridicat de risc furnizate digital se utilizează un marcaj CE digital numai dacă poate fi accesat cu ușurință prin intermediul interfeței de la care este accesat sistemul respectiv sau printr-un cod ușor accesibil, prelucrabil automat, sau prin alte mijloace electronice.

- (3) Marcajul CE se aplică în mod vizibil, lizibil și indelebil pe sistemele de IA cu grad ridicat de risc. În cazul în care acest lucru nu este posibil sau justificat din considerente ținând de natura sistemului de IA cu grad ridicat de risc, marcajul se aplică pe ambalaj sau pe documentele de însoțire, după caz.
- (4) Dacă este cazul, marcajul CE este urmat de numărul de identificare al organismului notificat responsabil de procedurile de evaluare a conformității menționate la articolul 43. Numărul de identificare al organismului notificat se aplică chiar de către organism sau, la instrucțiunile acestuia, de către furnizor sau reprezentantul autorizat al furnizorului. De asemenea, numărul de identificare se indică în orice material promoțional care menționează că sistemul de IA cu grad ridicat de risc îndeplinește cerințele aferente marcajului CE.
- (5) În cazul în care sistemele de IA cu grad ridicat de risc fac obiectul altor acte legislative ale Uniunii care prevăd de asemenea aplicarea marcajului CE, acesta indică faptul că sistemele de IA cu grad ridicat de risc îndeplinesc și cerințele celorlalte acte legislative.

Articolul 49

Înregistrare

- (1) Înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA cu grad ridicat de risc care figurează în anexa III, cu excepția sistemelor de IA cu grad ridicat de risc menționate în anexa III punctul 2, furnizorul și, după caz, reprezentantul autorizat se înregistrează pe sine, alături de sistemul lor în baza de date a UE menționată la articolul 71.

- (2) Înainte de a introduce pe piață sau de a pune în funcțiune un sistem de IA pentru care furnizorul a concluzionat că nu prezintă un grad ridicat de risc în conformitate cu articolul 6 alineatul (3), furnizorul respectiv sau, după caz, reprezentantul autorizat se înregistrează pe sine, alături de sistemul respectiv în baza de date a UE menționată la articolul 71.
- (3) Înainte de a pune în funcțiune sau de a utiliza un sistem de IA cu grad ridicat de risc care figurează în anexa III, cu excepția sistemelor de IA cu grad ridicat de risc care figurează în anexa III punctul 2, implementatorii care sunt autorități publice, instituții, organe, oficii sau agenții ale Uniunii ori persoane care acționează în numele acestora se înregistrează, selectează sistemul și înregistrează utilizarea acestuia în baza de date a UE menționată la articolul 71.
- (4) Pentru sistemele de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III, în domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontieră, înregistrarea menționată la alineatele (1), (2) și (3) de la prezentul articol se realizează în cadrul unei secțiuni securizate, care nu este accesibilă publicului, a bazei de date a UE menționate la articolul 71 și include numai următoarele informații, după caz, menționate la:
- (a) secțiunea A punctele 1-10 din anexa VIII, cu excepția punctelor 6, 8 și 9;
 - (b) secțiunea B punctele 1-5, 8 și 9 din anexa VIII;
 - (c) secțiunea C punctele 1-3 din anexa VIII;
 - (d) punctele 1, 2, 3 și 5 din anexa IX.

Numai Comisia și autoritățile naționale menționate la articolul 74 alineatul (8) au acces la secțiunile restricționate respective ale bazei de date a UE care figurează la primul paragraf de la prezentul alineat.

- (5) Sistemele de IA cu grad ridicat de risc menționate la punctul 2 din anexa III se înregistrează la nivel național.

Capitolul IV

Obligații de transparență pentru furnizorii și implementatorii anumitor sisteme de IA

Articolul 50

Obligații de transparență pentru furnizorii și implementatorii anumitor sisteme de IA

- (1) Furnizorii se asigură că sistemele de IA destinate să interacționeze direct cu persoane fizice sunt proiectate și dezvoltate astfel încât persoanele fizice în cauză să fie informate că interacționează cu un sistem de IA, cu excepția cazului în care acest lucru este evident din punctul de vedere al unei persoane fizice rezonabil de bine informată, de atentă și de avizată, ținând seama de circumstanțele și contextul de utilizare. Această obligație nu se aplică sistemelor de IA autorizate prin lege pentru a depista, a preveni, a investiga sau a urmări penal infracțiunile, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților, cu excepția cazului în care aceste sisteme sunt disponibile publicului pentru a denunța o infracțiune.

- (2) Furnizorii de sisteme de IA, inclusiv de sisteme de IA de uz general, care generează conținut sintetic în format audio, imagine, video sau text, se asigură că rezultatele sistemului de IA sunt marcate într-un format prelucrabil automat și detectabile ca fiind generate sau manipulate artificial. Furnizorii se asigură că soluțiile lor tehnice sunt eficace, interoperabile, solide și fiabile, în măsura în care acest lucru este fezabil din punct de vedere tehnic, ținând seama de particularitățile și limitările diferitelor tipuri de conținut, de costurile de punere în aplicare și de stadiul de avansare general recunoscut al tehnologiei, astfel cum poate fi reflectat în standardele tehnice relevante. Această obligație nu se aplică în măsura în care sistemele de IA îndeplinesc o funcție de asistare pentru editarea standard sau nu modifică în mod substanțial datele de intrare furnizate de implementator sau semantica acestora sau în cazul în care sunt autorizate prin lege să depisteze, să prevină, să investigheze sau să urmărească penal infracțiunile.
- (3) Implementatorii unui sistem de recunoaștere a emoțiilor sau ai unui sistem de clasificare biometrică informează persoanele fizice expuse sistemului respectiv cu privire la funcționarea acestuia și prelucrează datele cu caracter personal în conformitate cu Regulamentele (UE) 2016/679 și (UE) 2018/1725 și cu Directiva (UE) 2016/680, după caz. Această obligație nu se aplică sistemelor de IA utilizate pentru clasificarea biometrică și recunoașterea emoțiilor, care sunt autorizate prin lege să depisteze, să prevină sau să investigheze infracțiunile, sub rezerva unor garanții adecvate pentru drepturile și libertățile terților și în conformitate cu dreptul Uniunii.

- (4) Implementatorii unui sistem de IA care generează sau manipulează imagini, conținuturi audio sau video care constituie deepfake-uri dezvăluie faptul că respectivul conținut a fost generat sau manipulat artificial. Această obligație nu se aplică în cazul în care utilizarea este autorizată prin lege pentru depistarea, prevenirea, investigarea sau urmărirea penală a infracțiunilor. În cazul în care conținutul face parte dintr-o operă sau dintr-un program de o vădită natură artistică, creativă, satirică, fictivă sau analogă, obligațiile de transparență prevăzute la prezentul alineat se limitează la divulgarea existenței unui astfel de conținut generat sau manipulat într-un mod adecvat, care să nu împiedice afișarea sau receptarea operei.

Implementatorii unui sistem de IA care generează sau manipulează texte publicate cu scopul de a informa publicul cu privire la chestiuni de interes public dezvăluie faptul că textul a fost generat sau manipulat artificial. Această obligație nu se aplică în cazul în care utilizarea este autorizată prin lege pentru a depista, a preveni, a investiga sau a urmări penal infracțiunile sau în cazul în care conținutul generat de IA a fost supus unui proces de verificare editorială sau revizuire umană și responsabilitatea editorială pentru publicarea conținutului este deținută de o persoană fizică sau juridică.

- (5) Informațiile menționate la alineatele (1)-(4) sunt furnizate persoanelor fizice în cauză într-un mod clar și distinct, cel târziu în momentul primei interacțiuni sau al primei expuneri. Informațiile trebuie să respecte cerințele de accesibilitate aplicabile.
- (6) Alineatele (1)-(4) nu aduc atingere cerințelor și obligațiilor prevăzute în capitolul III și nici altor obligații de transparență pentru implementatorii de sisteme de IA prevăzute în dreptul Uniunii sau în dreptul intern.

- (7) Oficiul pentru IA încurajează și facilitează elaborarea de coduri de bune practici la nivelul Uniunii pentru a facilita punerea în aplicare efectivă a obligațiilor privind depistarea și etichetarea conținutului generat sau manipulat artificial. Comisia poate să adopte acte de punere în aplicare pentru a aproba respectivele coduri de bune practici în conformitate cu procedura prevăzută la articolul 56 alineatul (6). În cazul în care consideră că codul nu este adecvat, Comisia poate să adopte un act de punere în aplicare care să precizeze normele comune pentru punerea în aplicare a obligațiilor respective, în conformitate cu procedura de examinare prevăzută la articolul 98 alineatul (2).

Capitolul V

Modele de IA de uz general

SECȚIUNEA 1

NORME DE CLASIFICARE

Articolul 51

Clasificarea modelelor de IA de uz general ca modele de IA de uz general cu risc sistemic

- (1) Un model de IA de uz general este clasificat drept model de IA de uz general cu risc sistemic dacă îndeplinește oricare dintre următoarele condiții:
- (a) are capacități cu impact ridicat evaluate pe baza unor instrumente și metodologii tehnice adecvate, inclusiv a unor indicatori și valori de referință;

- (b) pe baza unei decizii a Comisiei, *ex officio* sau în urma unei alerte calificate din partea grupului științific, are capabilități sau un impact echivalente cu cele prevăzute la litera (a), având în vedere criteriile stabilite în anexa XIII.
- (2) Se consideră că un model de IA de uz general are capabilități cu impact ridicat în temeiul alineatului (1) litera (a) atunci când volumul cumulat de calcul utilizat pentru antrenarea sa măsurat în operații în virgulă mobilă este mai mare de 10^{25} .
- (3) Comisia adoptă acte delegate în conformitate cu articolul 97 pentru a modifica pragurile care figurează la alineatele (1) și (2) de la prezentul articol, precum și pentru a completa valorile de referință și indicatorii având în vedere evoluțiile tehnologice constante, cum ar fi îmbunătățirile algoritmice sau eficiența sporită a hardware-ului, atunci când este necesar, astfel încât pragurile respective să reflecte stadiul cel mai avansat al tehnologiei.

Articolul 52

Procedură

- (1) În cazul în care un model de IA de uz general îndeplinește condiția menționată la articolul 51 alineatul (1) litera (a), furnizorul relevant informează Comisia fără întârziere și, în orice caz, în termen de două săptămâni de la îndeplinirea cerinței respective sau de la data la care se constată faptul că va fi îndeplinită. Notificarea respectivă include informațiile necesare pentru a demonstra că a fost îndeplinită cerința relevantă. În cazul în care ia cunoștință de un model de IA de uz general care prezintă riscuri sistemice cu privire la care nu a fost notificată, Comisia poate decide să îl desemneze drept model prezentând risc sistemic.

- (2) Furnizorul unui model de IA de uz general care îndeplinește condiția menționată la articolul 51 alineatul (1) litera (a) poate prezenta, odată cu notificarea sa, argumente suficient de întemeiate pentru a demonstra că, în mod excepțional, deși îndeplinește cerința respectivă, modelul de IA de uz general nu prezintă riscuri sistemice, având în vedere caracteristicile sale specifice și, prin urmare, nu ar trebui să fie clasificat drept model de IA de uz general cu risc sistemic.
- (3) În cazul în care concluzionează că argumentele prezentate în temeiul alineatului (2) nu sunt suficient de întemeiate, iar furnizorul relevant nu a fost în măsură să demonstreze că modelul de IA de uz general nu prezintă riscuri sistemice, având în vedere caracteristicile sale specifice, Comisia respinge argumentele respective, iar modelul de IA de uz general este considerat un model de IA de uz general cu risc sistemic.
- (4) Comisia poate desemna un model de IA de uz general ca prezentând riscuri sistemice, *ex officio* sau în urma unei alerte calificate din partea grupului științific în temeiul articolului 90 alineatul (1) litera (a), pe baza criteriilor stabilite în anexa XIII.

Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a modifica anexa XIII prin precizarea și actualizarea criteriilor prevăzute în anexa menționată.

- (5) La cererea motivată a unui furnizor al cărui model a fost desemnat drept model de IA de uz general cu risc sistemic în temeiul alineatului (4), Comisia ia în considerare cererea și poate decide să reevalueze dacă modelul de IA de uz general poate fi considerat în continuare ca prezentând riscuri sistemice pe baza criteriilor prevăzute în anexa XIII. O astfel de cerere conține motive obiective, detaliate și noi care au survenit după decizia de desemnare. Furnizorii pot solicita reevaluarea cel mai devreme la șase luni de la decizia de desemnare. În cazul în care, în urma reevaluării sale, Comisia decide să mențină desemnarea drept model de IA de uz general cu risc sistemic, furnizorii pot solicita reevaluarea cel mai devreme la șase luni de la decizia respectivă.
- (6) Comisia se asigură că se publică o listă a modelelor de IA de uz general cu risc sistemic și actualizează lista respectivă, fără a aduce atingere necesității de a respecta și de a proteja drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale în conformitate cu dreptul Uniunii și cu dreptul intern.

SECȚIUNEA 2

OBLIGAȚIILE FURNIZORILOR DE MODELE DE IA DE UZ GENERAL

Articolul 53

Obligațiile furnizorilor de modele de IA de uz general

- (1) Furnizorii de sisteme de IA de uz general:
 - (a) realizează și actualizează documentația tehnică a modelului, inclusiv procesul vizând antrenarea și testarea sa, precum și rezultatele evaluării sale, care conțin cel puțin informațiile prevăzute în anexa XI în scopul de a le furniza, la cerere, Oficiului pentru IA și autorităților naționale competente;
 - (b) elaborează, actualizează și pun la dispoziție informații și documentație destinate furnizorilor de sisteme de IA care intenționează să integreze modelul de IA de uz general în sistemele lor de IA. Fără a aduce atingere necesității de a respecta și de a proteja drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale în conformitate cu dreptul Uniunii și cu dreptul intern, informațiile și documentația:
 - (i) le permit furnizorilor de sisteme de IA să înțeleagă bine capabilitățile și limitările modelului de IA de uz general și să respecte obligațiile care le revin în temeiul prezentului regulament; și
 - (ii) conțin cel puțin elementele prevăzute în anexa XII;

- (c) pun în aplicare o politică vizând respectarea dreptului Uniunii privind drepturile de autor și drepturile conexe și, în special, identificarea și respectarea, inclusiv pe baza stadiului cel mai avansat al tehnologiei, a unei rezervări a drepturilor exprimate în temeiul articolului 4 alineatul (3) din Directiva (UE) 2019/790;
 - (d) elaborează și pun la dispoziția publicului un rezumat suficient de detaliat cu privire la conținutul utilizat pentru antrenarea modelului de IA de uz general, în conformitate cu un model furnizat de Oficiul pentru IA.
- (2) Obligațiile prevăzute la alineatul (1) literele (a) și (b) nu se aplică furnizorilor de modele de IA care sunt lansate sub licență liberă și deschisă permițând accesul, utilizarea, modificarea și distribuția modelelor respective și ai căror parametri, inclusiv ponderile și informațiile privind arhitectura modelelor și utilizarea acestora, sunt puși la dispoziția publicului. Această excepție nu se aplică modelelor de IA de uz general cu risc sistemic.
- (3) Furnizorii de modele de IA de uz general cooperează, după caz, cu Comisia și cu autoritățile naționale competente în exercitarea competențelor și a prerogativelor lor în temeiul prezentului regulament.

- (4) Furnizorii de modele de IA de uz general se pot baza pe coduri de bune practici în sensul articolului 56 pentru a demonstra respectarea obligațiilor prevăzute la alineatul (1) de la prezentul articol, până la publicarea unui standard armonizat. Respectarea standardelor europene armonizate oferă furnizorilor prezumția de conformitate, în măsura în care standardele respective vizează obligațiile respective. Furnizorii de modele de IA de uz general care nu aderă la un cod de bune practici aprobat sau nu respectă un standard european armonizat demonstrează existența unor mijloace alternative adecvate de conformitate spre a fi evaluate de Comisie.
- (5) În scopul facilitării respectării anexei XI, în special a punctului 2 literele (d) și (e), Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 pentru a detalia metodologiile de măsurare și de calculare, astfel încât documentațiile să poată fi comparabile și verificabile.
- (6) Comisia este împuternicită să adopte acte delegate în conformitate cu articolul 97 alineatul (2) pentru a modifica anexele XI și XII având în vedere evoluțiile tehnologice constante.
- (7) Orice informații sau documentație obținute în temeiul prezentului articol, inclusiv secretele comerciale, sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 54

Reprezentanții autorizați ai furnizorilor de modele de IA de uz general

- (1) Înainte de a pune la dispoziție un model de IA de uz general pe piața Uniunii, furnizorii stabiliți în țări terțe desemnează, prin mandat scris, un reprezentant autorizat stabilit în Uniune.

- (2) Furnizorul permite reprezentantului său autorizat să îndeplinească sarcinile prevăzute în mandatul primit de la furnizor.
- (3) Reprezentantul autorizat îndeplinește sarcinile prevăzute în mandatul primit de la furnizor. Acesta furnizează Oficiului pentru IA, la cerere, o copie a mandatului, într-una din limbile oficiale ale instituțiilor Uniunii. În sensul prezentului regulament, mandatul îl împuternicește pe reprezentantul autorizat să îndeplinească următoarele sarcini:
- (a) să verifice dacă a fost întocmită documentația tehnică specificată în anexa XI și dacă au fost îndeplinite de către furnizor toate obligațiile menționate la articolul 53 și, după caz, la articolul 55;
 - (b) să păstreze la dispoziția Oficiului pentru IA și a autorităților naționale competente o copie a documentației tehnice specificate în anexa XI pentru o perioadă de 10 ani după introducerea pe piață a modelului de IA de uz general, precum și datele de contact ale furnizorului care a desemnat reprezentantul autorizat;
 - (c) să furnizeze Oficiului pentru IA, în urma unei cereri motivate, toate informațiile și documentația, inclusiv cele menționate la litera (b), necesare pentru a demonstra respectarea de către furnizor a obligațiilor prevăzute în prezentul capitol;
 - (d) să coopereze cu Oficiul pentru IA și cu autoritățile competente, în urma unei cereri motivate, cu privire la orice acțiune întreprinsă de acestea în legătură cu un model de IA de uz general, inclusiv atunci când modelul este integrat în sistemele de IA introduse pe piață sau puse în funcțiune în Uniune.

- (4) Mandatul împuternicește reprezentantul autorizat să fie contactat, pe lângă furnizor sau în locul acestuia, de către Oficiul pentru IA sau autoritățile competente, cu referire la toate aspectele legate de asigurarea conformității cu prezentul regulament.
- (5) Reprezentantul autorizat își reziliază mandatul dacă consideră sau are motive să considere că furnizorul acționează contrar obligațiilor care îi revin în temeiul prezentului regulament. Într-un astfel de caz, el informează imediat Oficiul pentru IA cu privire la rezilierea mandatului și la motivele acesteia.
- (6) Obligația prevăzută la prezentul articol nu se aplică furnizorilor de modele de IA de uz general care sunt lansate sub licență liberă și cu sursă deschisă permițând accesul, utilizarea, modificarea și distribuția modelelor respective și ai căror parametri, inclusiv ponderile și informațiile privind arhitectura modelelor și utilizarea acestora, sunt puși la dispoziția publicului, cu excepția cazului în care modelele de IA de uz general prezintă riscuri sistemice.

SECȚIUNEA 3
OBLIGAȚIILE FURNIZORILOR DE MODELE DE IA DE UZ GENERAL
CU RISC SISTEMIC

Articolul 55

Obligațiile furnizorilor de modele de IA de uz general cu risc sistemic

- (1) Pe lângă obligațiile enumerate la articolele 53 și 54, furnizorii de modele de IA de uz general cu risc sistemic:
- (a) efectuează evaluarea modelelor în conformitate cu protocoale și instrumente standardizate care reflectă stadiul de avansare al tehnologiei, inclusiv prin efectuarea de testări contradictorii ale modelelor și documentarea acestora, în vederea identificării și atenuării riscurilor sistemice;
 - (b) evaluează și atenuează posibilele riscuri sistemice la nivelul Uniunii, inclusiv sursele acestora, care pot decurge din dezvoltarea, introducerea pe piață sau utilizarea unor modele de IA de uz general cu risc sistemic;
 - (c) urmăresc, documentează și raportează fără întârzieri nejustificate Oficiului pentru IA și, după caz, autorităților naționale competente, informații relevante cu privire la incidentele grave și la posibilele măsuri corective pentru a le aborda;
 - (d) asigură un nivel adecvat de protecție a securității cibernetice pentru modelele de IA de uz general cu risc sistemic și pentru infrastructura fizică a modelelor.

- (2) Furnizorii de modele de IA de uz general cu risc sistemic se pot baza pe coduri de bune practici în sensul articolului 56 pentru a demonstra respectarea obligațiilor prevăzute la alineatul (1) de la prezentul articol, până la publicarea unui standard armonizat. Respectarea standardelor europene armonizate oferă furnizorilor prezumția de conformitate, în măsura în care standardele respective vizează obligațiile respective. Furnizorii de modele de IA de uz general cu risc sistemic care nu aderă la un cod de bune practici aprobat sau nu respectă un standard european armonizat demonstrează existența unor mijloace alternative adecvate de conformitate, spre a fi evaluate de Comisie.
- (3) Orice informații sau documentație obținute în temeiul prezentului articol, inclusiv secretele comerciale, sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

SECȚIUNEA 4

CODURI DE BUNE PRACTICI

Articolul 56

Coduri de bune practici

- (1) Oficiul pentru IA încurajează și facilitează elaborarea de coduri de bune practici la nivelul Uniunii pentru a contribui la aplicarea corespunzătoare a prezentului regulament, ținând seama de abordările internaționale.

- (2) Oficiul pentru IA și Consiliul IA urmăresc să se asigure că codurile de bune practici vizează cel puțin obligațiile prevăzute la articolele 53 și 55, inclusiv următoarele aspecte:
- (a) mijloacele de asigurare a faptului că informațiile menționate la articolul 53 alineatul (1) literele (a) și (b) sunt actualizate având în vedere evoluțiile tehnologice și ale pieței;
 - (b) nivelul adecvat de detaliere a rezumatului cu privire la conținutul utilizat pentru antrenare;
 - (c) identificarea tipului și naturii riscurilor sistemice la nivelul Uniunii, inclusiv a surselor acestora, după caz;
 - (d) măsurile, procedurile și modalitățile pentru evaluarea și gestionarea riscurilor sistemice la nivelul Uniunii, inclusiv documentația aferentă, care sunt proporționale cu riscurile, iau în considerare gravitatea și probabilitatea acestora, precum și provocările specifice legate de abordarea acestor riscuri, având în vedere modurile posibile în care astfel de riscuri pot apărea și se pot materializa de-a lungul lanțului valoric al IA.
- (3) Oficiul pentru IA poate invita toți furnizorii de modele de IA de uz general, precum și autoritățile naționale competente relevante, să participe la elaborarea de coduri de bune practici. Organizațiile societății civile, industria, mediul academic și alte părți interesate relevante, cum ar fi furnizorii din aval și experții independenți, pot sprijini procesul.

- (4) Oficiul pentru IA și Consiliul IA urmăresc să se asigure că codurile de bune practici stabilesc în mod clar obiectivele lor specifice, conțin angajamente sau măsuri, inclusiv indicatori-cheie de performanță, după caz, pentru a asigura realizarea obiectivelor respective și că acestea țin seama în mod corespunzător de nevoile și interesele tuturor părților interesate, inclusiv ale persoanelor afectate, la nivelul Uniunii.
- (5) Oficiul pentru IA urmărește să se asigure că participanții la codurile de bune practici raportează periodic Oficiului pentru IA cu privire la punerea în aplicare a angajamentelor și a măsurilor luate și a rezultatelor acestora, inclusiv astfel cum sunt măsurate în raport cu indicatorii-cheie de performanță, după caz. Indicatorii-cheie de performanță și obligațiile de raportare reflectă diferențele de dimensiune și de capacitate dintre diferiții participanți.
- (6) Oficiul pentru IA și Consiliul IA monitorizează și evaluează periodic îndeplinirea obiectivelor codurilor de bune practici de către participanți și contribuția acestora la aplicarea corespunzătoare a prezentului regulament. Oficiul pentru IA și Consiliul IA evaluează dacă codurile de bune practici vizează obligațiile prevăzute la articolele 53 și 55 și monitorizează și evaluează periodic îndeplinirea obiectivelor lor. Acestea publică evaluarea caracterului adecvat al codurilor de bune practici.

Comisia poate, prin intermediul unui act de punere în aplicare, să aprobe un cod de bune practici și îi poate conferi o valabilitate generală în cadrul Uniunii. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

- (7) Oficiul pentru IA poate invita toți furnizorii de modele de IA de uz general să adere la codurile de bune practici. Pentru furnizorii de modele de IA de uz general care nu prezintă riscuri sistemice, aderarea respectivă se poate limita la obligațiile prevăzute la articolul 53, cu excepția cazului în care aceștia își declară în mod explicit interesul de a adera la codul integral.
- (8) De asemenea, Oficiul pentru IA încurajează și facilitează, după caz, revizuirea și adaptarea codurilor de bune practici, în special în lumina standardelor emergente. Oficiul pentru IA contribuie la evaluarea standardelor disponibile.
- (9) Codurile de bune practici sunt pregătite cel târziu până la ... [nouă luni de la data intrării în vigoare a prezentului regulament]. Oficiul pentru IA face demersurile necesare, inclusiv prin invitarea furnizorilor în temeiul alineatului (7).

În cazul în care, până la ... [12 luni de la data intrării în vigoare], nu poate fi finalizat un cod de bune practici sau în cazul în care Oficiul pentru IA consideră, în urma evaluării sale în temeiul alineatului (6) de la prezentul articol, că acesta nu este adecvat, Comisia poate prevedea, prin intermediul unor acte de punere în aplicare, norme comune pentru punerea în aplicare a obligațiilor prevăzute la articolele 53 și 55, inclusiv aspectele prevăzute la alineatul (2) de la prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Capitolul VI

Măsuri de sprijinire a inovării

Articolul 57

Spațiile de testare în materie de reglementare în domeniul IA

- (1) Statele membre se asigură că autoritățile lor competente instituie cel puțin un spațiu de testare în materie de reglementare în domeniul IA la nivel național, care este operațional până la ... [24 de luni de la data intrării în vigoare a prezentului regulament]. Spațiul de testare respectiv poate fi instituit, de asemenea, împreună cu autoritățile competente din alte state membre. Comisia poate oferi sprijin tehnic, consiliere și instrumente pentru instituirea și exploatarea spațiilor de testare în materie de reglementare în domeniul IA.

Obligația prevăzută la primul paragraf poate fi îndeplinită și prin participarea la un spațiu de testare existent, în măsura în care această participare asigură un nivel echivalent de acoperire națională pentru statele membre participante.

- (2) De asemenea, pot fi instituite spații de testare suplimentare în materie de reglementare în domeniul IA la nivel regional sau local sau împreună cu autoritățile competente din alte state membre.
- (3) Autoritatea Europeană pentru Protecția Datelor poate, de asemenea, să instituie un spațiu de testare în materie de reglementare în domeniul IA pentru instituțiile, organele, oficiile și agențiile Uniunii și poate să exercite rolurile și sarcinile autorităților naționale competente în conformitate cu prezentul capitol.

- (4) Statele membre se asigură că autoritățile competente menționate la alineatele (1) și (2) alocă resurse suficiente pentru a se conforma prezentului articol în mod eficace și în timp util. După caz, autoritățile naționale competente cooperează cu alte autorități relevante și pot permite implicarea altor actori din ecosistemul de IA. Prezentul articol nu aduce atingere altor spații de testare în materie de reglementare instituite în temeiul dreptului Uniunii sau al dreptului intern. Statele membre asigură un nivel adecvat de cooperare între autoritățile care supraveghează aceste alte spații de testare și autoritățile naționale competente.
- (5) Spațiile de testare în materie de reglementare în domeniul IA instituite în temeiul alineatului (1) prevăd un mediu controlat care promovează inovarea și facilitează dezvoltarea, antrenare, testarea și validarea sistemelor de IA inovatoare pentru o perioadă limitată de timp înainte de introducerea lor pe piață sau de punerea lor în funcțiune în temeiul unui plan specific privind spațiul de testare convenit între furnizori sau furnizorii potențiali și autoritatea competentă. Astfel de spații de testare pot include testarea în condiții reale supravegheată în spațiul de testare.
- (6) Autoritățile competente oferă, după caz, orientări, supraveghere și sprijin în cadrul spațiului de testare în materie de reglementare în domeniul IA în vederea identificării riscurilor, în special în ceea ce privește drepturile fundamentale, sănătatea și siguranța, în vederea testării, precum și în vederea unor măsuri de atenuare și a asigurării eficacității acestora în ceea ce privește obligațiile și cerințele prezentului regulament și, după caz, ale altor dispoziții din dreptul Uniunii și dreptul intern care fac obiectul supravegherii în cadrul spațiului de testare.
- (7) Autoritățile competente oferă furnizorilor și potențialilor furnizori care participă la spațiul de testare în materie de reglementare în domeniul IA orientări privind așteptările în materie de reglementare și modul de îndeplinire a cerințelor și a obligațiilor prevăzute în prezentul regulament.

La cererea furnizorului sau a potențialului furnizor al sistemului de IA, autoritatea competentă furnizează o dovadă scrisă a activităților desfășurate cu succes în spațiul de testare. Autoritatea competentă furnizează, de asemenea, un raport de ieșire care detaliază activitățile desfășurate în spațiul de testare, precum și realizările și rezultatele învățării aferente. Furnizorii pot utiliza o astfel de documentație pentru a demonstra că respectă prezentul regulament prin intermediul procesului de evaluare a conformității sau al activităților relevante de supraveghere a pieței. În acest sens, rapoartele de ieșire și dovezile scrise furnizate de autoritatea națională competentă sunt luate în considerare în mod pozitiv de către autoritățile de supraveghere a pieței și de către organismele notificate, în vederea accelerării procedurilor de evaluare a conformității într-o măsură rezonabilă.

- (8) Sub rezerva dispozițiilor privind confidențialitatea de la articolul 78 și cu acordul furnizorului sau al potențialului furnizor, Comisia și Consiliul IA sunt autorizate să acceseze rapoartele de ieșire și le iau în considerare, după caz, atunci când își exercită atribuțiile în temeiul prezentului regulament. Dacă atât furnizorul sau potențialul furnizor, cât și autoritatea națională competentă își dau acordul în mod explicit, raportul de ieșire poate fi pus la dispoziția publicului prin intermediul platformei unice de informare menționate la prezentul articol.
- (9) Instituirea spațiilor de testare în materie de reglementare în domeniul IA urmărește să contribuie la următoarele obiective:
- (a) îmbunătățirea securității juridice pentru a asigura conformitatea normativă cu prezentul regulament sau, după caz, cu alte dispoziții aplicabile din dreptul Uniunii și din dreptul intern;
 - (b) sprijinirea schimbului de bune practici prin cooperarea cu autoritățile implicate în spațiul de testare în materie de reglementare în domeniul IA;

- (c) stimularea inovării și a competitivității și facilitarea dezvoltării unui ecosistem de IA;
 - (d) furnizarea de contribuții la învățarea bazată pe dovezi în materie de reglementare;
 - (e) facilitarea și accelerarea accesului la piața Uniunii pentru sistemele de IA, în special atunci când sunt furnizate de IMM-uri, inclusiv de întreprinderi nou-înființate.
- (10) Autoritățile naționale competente se asigură că, în măsura în care sistemele de IA inovatoare implică prelucrarea de date cu caracter personal sau aparțin în alt mod competenței de supraveghere a altor autorități naționale sau autorități competente care furnizează sau sprijină accesul la date, autoritățile naționale de protecție a datelor sau celelalte autorități naționale sau competente respective sunt asociate exploatării spațiului de testare în materie de reglementare în domeniul IA și sunt implicate în supravegherea aspectelor respective pe măsura sarcinilor și a competențelor lor respective.
- (11) Spațiile de testare în materie de reglementare în domeniul IA nu afectează competențele de supraveghere sau atribuțiile corective ale autorităților competente care supraveghează spațiile de testare, inclusiv la nivel regional sau local. Orice riscuri semnificative pentru sănătate, siguranță și drepturile fundamentale identificate în timpul dezvoltării și testării unor astfel de sisteme de IA conduc la o atenuare adecvată. Autoritățile naționale competente au competența de a suspenda temporar sau permanent procesul de testare sau participarea la spațiul de testare dacă nu este posibilă o atenuare eficientă și informează Oficiul pentru IA cu privire la o astfel de decizie. Autoritățile naționale competente își exercită competențele de supraveghere în limitele dreptului relevant, utilizându-și competențele discreționare atunci când pun în aplicare dispoziții juridice pentru un anumit proiect de spațiu de testare în materie de reglementare în domeniul IA, cu obiectivul de a sprijini inovarea în domeniul IA în Uniune.

- (12) Furnizorii și potențialii furnizori care participă la spațiul de testare în materie de reglementare în domeniul IA rămân responsabili, în temeiul dreptului aplicabil al Uniunii și al dreptului național aplicabil în materie de răspundere, pentru orice prejudiciu adus terților ca urmare a experimentării care are loc în spațiul de testare. Cu toate acestea, cu condiția ca potențialii furnizori să respecte planul specific și termenele și condițiile pentru participarea lor și să urmeze cu bună-credință orientările oferite de autoritatea națională competentă, autoritățile nu impun amenzi administrative pentru încălcarea prezentului regulament. În cazurile în care în supravegherea sistemului de IA în spațiul de testare au mai fost implicate activ și alte autorități competente, responsabile de alte dispoziții ale dreptului Uniunii și ale dreptului intern, care au furnizat orientări pentru conformitate, nu se impun amenzi administrative în ceea ce privește actele legislative respective.
- (13) Spațiile de testare în materie de reglementare în domeniul IA sunt concepute și puse în aplicare astfel încât, după caz, să faciliteze cooperarea transfrontalieră între autoritățile naționale competente.
- (14) Autoritățile naționale competente își coordonează activitățile și cooperează în cadrul Consiliului IA.
- (15) Autoritățile naționale competente informează Oficiul pentru IA și Consiliul IA cu privire la instituirea unui spațiu de testare și le pot solicita sprijin și orientări. Oficiul pentru IA pune la dispoziția publicului o listă a spațiilor de testare planificate și existente și o actualizează pentru a încuraja o mai mare interacțiune în spațiile de testare în materie de reglementare în domeniul IA, precum și cooperarea transfrontalieră.

- (16) Autoritățile naționale competente prezintă rapoarte anuale Oficiului pentru IA și Consiliului IA, începând cu un an de la instituirea spațiului de testare în materie de reglementare în domeniul IA și, ulterior, în fiecare an, până la încetarea acestuia, precum și un raport final. Rapoartele respective furnizează informații cu privire la progresele și rezultatele punerii în aplicare a spațiilor de testare respective, inclusiv cu privire la bune practici, incidente, lecții învățate și recomandări privind instituirea acestora și, după caz, cu privire la aplicarea și posibila revizuire a prezentului regulament, inclusiv a actelor sale delegate și de punere în aplicare, precum și cu privire la aplicarea altor dispoziții de drept ale Uniunii sub supravegherea autorităților competente în spațiul de testare. Autoritățile naționale competente pun la dispoziția publicului, online, rapoartele anuale respective sau rezumate ale acestora. Comisia ține seama, după caz, de rapoartele anuale atunci când își exercită atribuțiile în temeiul prezentului regulament.
- (17) Comisia dezvoltă o interfață unică și specifică în cadrul căreia sunt reunite toate informațiile relevante legate de spațiile de testare în materie de reglementare în domeniul IA pentru a permite părților interesate să interacționeze cu spațiile de testare în materie de reglementare în domeniul IA, să adreseze întrebări autorităților competente și să solicite orientări fără caracter obligatoriu cu privire la conformitatea produselor, a serviciilor și a modelelor de afaceri inovatoare care încorporează tehnologii de IA, în conformitate cu articolul 62 alineatul (1) litera (c). Comisia se coordonează în mod proactiv cu autoritățile naționale competente, după caz.

Articolul 58

Modalități detaliate privind spațiile de testare în materie de reglementare a IA și funcționarea acestora

- (1) Pentru a evita fragmentarea în cadrul Uniunii, Comisia adoptă acte de punere în aplicare care precizează modalitățile detaliate de instituire, dezvoltare, punere în aplicare, exploatare și supraveghere a spațiilor de testare în materie de reglementare în domeniul IA. Actele de punere în aplicare includ principii comune cu privire la următoarele aspecte:
- (a) criteriile de eligibilitate și de selecție pentru participarea la spațiul de testare în materie de reglementare în domeniul IA;
 - (b) procedurile de depunere a cererii, de participare, de monitorizare, de ieșire și de încetare în ceea ce privește spațiul de testare în materie de reglementare în domeniul IA, inclusiv planul privind spațiul de testare și raportul de ieșire;
 - (c) termenele și condițiile aplicabile participanților.

Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

- (2) Actele de punere în aplicare menționate la alineatul (1) garantează că:
- (a) spațiile de testare în materie de reglementare în domeniul IA sunt deschise oricărui furnizor sau potențial furnizor al unui sistem de IA care solicită accesul și care îndeplinește criteriile de eligibilitate și de selecție, care sunt transparente și echitabile, și că autoritățile naționale competente informează solicitanții cu privire la decizia lor în termen de trei luni de la depunerea cererii;

- (b) spațiile de testare în materie de reglementare în domeniul IA permit un acces larg și egal și țin pasul cu nivelul cererii în ceea ce privește participarea; furnizorii și potențialii furnizori pot, de asemenea, depune cereri în parteneriat cu implementatorii și alte părți terțe relevante;
- (c) modalitățile și condițiile detaliate privind spațiile de testare în materie de reglementare în domeniul IA sprijină, în cea mai mare măsură posibilă, flexibilitatea pentru ca autoritățile naționale competente să instituie și să exploateze spațiile lor de testare în materie de reglementare în domeniul IA;
- (d) accesul la spațiile de testare în materie de reglementare în domeniul IA este gratuit pentru IMM-uri, inclusiv întreprinderile nou-înființate, fără a aduce atingere costurilor excepționale pe care autoritățile naționale competente le pot recupera în mod echitabil și proporțional;
- (e) facilitează respectarea de către furnizori și potențialii furnizori, prin intermediul rezultatelor învățării din spațiile de testare în materie de reglementare în domeniul IA, a obligațiilor de evaluare a conformității în temeiul prezentului regulament și aplicarea voluntară de către aceștia a codurilor de conduită menționate la articolul 95;
- (f) spațiile de testare în materie de reglementare în domeniul IA facilitează implicarea altor actori relevanți din ecosistemul IA, cum ar fi organismele notificate și organizațiile de standardizare, IMM-urile, inclusiv întreprinderile nou-înființate, întreprinderile, inovatorii, instalațiile de testare și experimentare, laboratoarele de cercetare și experimentare și centrele europene de inovare digitală, centrele de excelență, cercetătorii individuali, pentru a permite și a facilita cooperarea cu sectorul public și cu sectorul privat;

- (g) procedurile, procesele și cerințele administrative pentru depunerea cererilor, selecție, participare și ieșirea din spațiul de testare în materie de reglementare în domeniul IA sunt simple, ușor de înțeles și comunicate în mod clar pentru a facilita participarea IMM-urilor, inclusiv a întreprinderilor nou-înființate, cu capacități juridice și administrative limitate și sunt raționalizate în întreaga Uniune, pentru a evita fragmentarea și astfel încât participarea la un spațiu de testare în materie de reglementare în domeniul IA instituit de un stat membru sau de Autoritatea Europeană pentru Protecția Datelor să fie recunoscută reciproc și uniform și să producă aceleași efecte juridice în întreaga Uniune;
 - (h) participarea la spațiul de testare în materie de reglementare în domeniul IA este limitată la o perioadă adecvată complexității și amplitudinii proiectului, și că poate fi prelungită de autoritatea națională competentă;
 - (i) spațiile de testare în materie de reglementare în domeniul IA facilitează dezvoltarea de instrumente și de infrastructură pentru testarea, etalonarea, evaluarea și explicarea dimensiunilor sistemelor de IA relevante pentru învățarea în materie de reglementare, cum ar fi acuratețea, robustețea și securitatea cibernetică, precum și de măsuri vizând reducerea riscurilor pentru drepturile fundamentale și pentru societate în general.
- (3) Potențialii furnizori din spațiile de testare în materie de reglementare în domeniul IA, în special IMM-urile și întreprinderile nou-înființate, sunt direcționați, după caz, către servicii de preimplementare, cum ar fi orientări privind punerea în aplicare a prezentului regulament, către alte servicii cu valoare adăugată, cum ar fi ajutorul acordat în privința documentelor de standardizare și a certificării, instalațiile de testare și experimentare, centrele europene de inovare digitală și centrele de excelență.

- (4) Atunci când autoritățile naționale competente iau în considerare autorizarea testării în condiții reale supravegheate în cadrul unui spațiu de testare în materie de reglementare în domeniul IA care urmează a fi instituit în temeiul prezentului articol, acestea convin în mod specific cu participanții asupra clauzelor și condițiilor unei astfel de testări și, în special, asupra garanțiilor adecvate în vederea protejării drepturilor fundamentale, a sănătății și a siguranței. După caz, acestea cooperează cu alte autorități naționale competente în vederea asigurării unor practici coerente în întreaga Uniune.

Articolul 59

Prelucrarea ulterioară a datelor cu caracter personal

în vederea dezvoltării anumitor sisteme de IA în interes public

în spațiul de testare în materie de reglementare în domeniul IA

- (1) În spațiul de testare în materie de reglementare în domeniul IA, datele cu caracter personal colectate în mod legal în alte scopuri pot fi prelucrate numai în scopul dezvoltării, antrenării și testării anumitor sisteme de IA în spațiul de testare, dacă sunt îndeplinite toate condițiile următoare:
- (a) sistemele de IA sunt dezvoltate pentru protejarea unui interes public substanțial de către o autoritate publică sau de către o altă persoană fizică sau juridică și în unul sau mai multe dintre următoarele domenii:
- (i) siguranța și sănătatea publică, inclusiv depistarea, diagnosticarea, prevenirea, controlul și tratarea bolilor și îmbunătățirea sistemelor de sănătate;
- (ii) un nivel ridicat de protejare și de îmbunătățire a calității mediului, protejarea biodiversității, protecția împotriva poluării, măsuri privind tranziția verde, măsuri privind atenuarea schimbărilor climatice și adaptarea la acestea;

- (iii) durabilitatea energetică;
 - (iv) siguranța și reziliența sistemelor de transport și a mobilității, a infrastructurii critice și a rețelelor;
 - (v) eficiența și calitatea administrației publice și a serviciilor publice;
- (b) datele prelucrate sunt necesare pentru a respecta una sau mai multe dintre cerințele menționate în capitolul III secțiunea 2, în cazul în care cerințele respective nu pot fi îndeplinite în mod eficace prin prelucrarea datelor anonimizate ori sintetice sau a altor date fără caracter personal;
- (c) există mecanisme eficace de monitorizare pentru a constata dacă în timpul experimentării în spațiul de testare pot apărea riscuri ridicate la adresa drepturilor și libertăților persoanelor vizate, astfel cum se menționează la articolul 35 din Regulamentul (UE) 2016/679 și la articolul 39 din Regulamentul (UE) 2018/1725, precum și mecanisme de răspuns pentru a atenua cu promptitudine aceste riscuri și, dacă este necesar, pentru a opri prelucrarea;
- (d) toate datele cu caracter personal care urmează să fie prelucrate în contextul spațiului de testare se află într-un mediu de prelucrare a datelor separat din punct de vedere funcțional, izolat și protejat, aflat sub controlul potențialului furnizor și numai persoanele autorizate au acces la datele respective;
- (e) furnizorii pot partaja ulterior datele colectate inițial numai în conformitate cu dreptul Uniunii în materie de protecție a datelor; datele cu caracter personal create în spațiul de testare nu pot fi partajate în afara spațiului de testare;

- (f) nicio prelucrare a datelor cu caracter personal în contextul spațiului de testare nu conduce la măsuri sau la decizii care afectează persoanele vizate și nici nu afectează aplicarea drepturilor acestora prevăzute în dreptul Uniunii privind protecția datelor cu caracter personal;
- (g) toate datele cu caracter personal prelucrate în contextul spațiului de testare sunt protejate prin măsuri tehnice și organizatorice adecvate și sunt șterse după ce participarea la spațiul respectiv a încetat sau datele cu caracter personal au ajuns la sfârșitul perioadei de păstrare;
- (h) fișierele de jurnalizare a prelucrării datelor cu caracter personal în contextul spațiului de testare sunt păstrate pe durata participării la spațiul de testare, în afara cazului în care există dispoziții diferite în dreptul Uniunii sau în dreptul intern;
- (i) descrierea completă și detaliată a procesului și a motivelor care stau la baza antrenării, testării și validării sistemului de IA este păstrată împreună cu rezultatele testelor, ca parte a documentației tehnice menționate în anexa IV;
- (j) pe site-ul web al autorităților competente sunt publicate un scurt rezumat al proiectului în materie de IA elaborat în spațiul de testare, precum și obiectivele și rezultatele preconizate ale acestuia; această obligație nu vizează datele operaționale sensibile legate de activitățile autorităților de aplicare a legii, de control la frontiere, de imigrație sau de azil.

- (2) În scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, sub controlul și responsabilitatea autorităților de aplicare a legii, prelucrarea datelor cu caracter personal în spațiile de testare în materie de reglementare în domeniul IA se bazează pe dispoziții specifice ale dreptului Uniunii sau ale dreptului intern și face obiectul acelorași condiții cumulative ca cele menționate la alineatul (1).
- (3) Alineatul (1) nu aduce atingere dreptului Uniunii sau dreptului intern care exclude prelucrarea datelor cu caracter personal în alte scopuri decât cele menționate în mod explicit în dreptul respectiv, precum și dreptului Uniunii sau dreptului intern care stabilește temeiul pentru prelucrarea datelor cu caracter personal care este necesară în scopul dezvoltării, testării sau antrenării sistemelor de IA inovatoare sau orice alt temei juridic, în conformitate cu dreptul Uniunii privind protecția datelor cu caracter personal.

Articolul 60

Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în afara spațiilor de testare în materie de reglementare în domeniul IA

- (1) Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în afara spațiilor de testare în materie de reglementare în domeniul IA poate fi efectuată de către furnizorii sau potențialii furnizori de sisteme de IA cu grad ridicat de risc enumerați în anexa III, în conformitate cu prezentul articol și cu planul de testare în condiții reale menționat în cadrul acestuia, fără a aduce atingere interdicțiilor prevăzute la articolul 5.

Comisia precizează, prin intermediul unor acte de punere în aplicare, elementele detaliate ale planului de testare în condiții reale. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Prezentul alineat nu aduce atingere dreptului Uniunii sau dreptului intern privind testarea în condiții reale a sistemelor de IA cu grad ridicat de risc legate de produsele care fac obiectul actelor legislative enumerate în anexa I.

- (2) Furnizorii sau potențialii furnizori pot efectua teste ale sistemelor de IA cu grad ridicat de risc menționate în anexa III în condiții reale în orice moment înainte de introducerea pe piață sau de punerea în funcțiune a sistemelor de IA pe cont propriu sau în parteneriat cu unul sau mai mulți implementatori sau implementatori potențiali.
- (3) Testarea sistemelor de IA cu grad ridicat de risc în condiții reale în temeiul prezentului articol nu aduce atingere oricărei evaluări etice care este impusă de dreptul Uniunii sau de dreptul intern.
- (4) Furnizorii sau potențialii furnizori pot efectua testarea în condiții reale numai dacă sunt îndeplinite toate condițiile următoare:
 - (a) furnizorul sau potențialul furnizor a elaborat un plan de testare în condiții reale și l-a prezentat autorității de supraveghere a pieței din statul membru în care urmează să se efectueze testarea în condiții reale;
 - (b) autoritatea de supraveghere a pieței din statul membru în care urmează să fie efectuată testarea în condiții reale a aprobat testarea în condiții reale și planul de testare în condiții reale; în cazul în care autoritatea de supraveghere a pieței nu a furnizat un răspuns în termen de 30 de zile, se consideră că testarea în condiții reale și planul de testare în condiții reale au fost aprobate; în cazul în care dreptul intern nu prevede o aprobare tacită, testarea în condiții reale face în continuare obiectul unei autorizații;

- (c) furnizorul sau potențialul furnizor, cu excepția furnizorului sau a potențialului furnizor de sisteme de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III în domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere și de sisteme de IA cu grad ridicat de risc menționate la punctul 2 din anexa III, a înregistrat testarea în condiții reale în conformitate cu articolul 71 alineatul (4) cu un număr unic de identificare la nivelul întregii Uniuni și furnizând informațiile specificate în anexa IX; furnizorul sau potențialul furnizor de sisteme de IA cu grad ridicat de risc menționate la punctele 1, 6 și 7 din anexa III în domeniul aplicării legii, al migrației, al azilului și al gestionării controlului la frontiere a înregistrat testarea în condiții reale în secțiunea securizată care nu este accesibilă publicului a bazei de date a UE în conformitate cu articolul 49 alineatul (4) litera (d), cu un număr unic de identificare la nivelul întregii Uniuni și furnizând informațiile specificate în acesta; furnizorul sau potențialul furnizor de sisteme de IA cu grad ridicat de risc menționate la punctul 2 din anexa III a înregistrat testarea în condiții reale în conformitate cu articolul 49 alineatul (5);
- (d) furnizorul sau potențialul furnizor care efectuează testarea în condiții reale este stabilit în Uniune sau a desemnat un reprezentant legal care este stabilit în Uniune;
- (e) datele colectate și prelucrate în scopul testării în condiții reale se transferă către țări terțe numai cu condiția implementării unor garanții corespunzătoare și aplicabile în temeiul dreptului Uniunii;

- (f) testarea în condiții reale nu durează mai mult decât este necesar pentru realizarea obiectivelor sale și, în orice caz, nu depășește o perioadă de 6 luni, care poate fi prelungită cu încă 6 luni, sub rezerva notificării prealabile de către furnizor sau potențialul furnizor a autorității de supraveghere a pieței, însoțită de o explicație privind necesitatea unei astfel de prelungiri;
- (g) subiecții testării în condiții reale, care sunt persoane care aparțin grupurilor vulnerabile din cauza vârstei sau a dizabilității, sunt protejați în mod corespunzător;
- (h) în cazul în care un furnizor sau un potențial furnizor organizează testarea în condiții reale în cooperare cu unul sau mai mulți implementatori sau implementatori potențiali, aceștia din urmă au fost informați cu privire la toate aspectele testării care sunt relevante pentru decizia lor de a participa și au primit instrucțiunile relevante pentru utilizarea sistemului de IA menționate la articolul 13; furnizorul sau potențialul furnizor și implementatorul sau potențialul implementator încheie un acord în care precizează rolurile și responsabilitățile lor, în vederea asigurării conformității cu dispozițiile privind testarea în condiții reale în temeiul prezentului regulament și al altor acte legislative aplicabile ale Uniunii, precum și al dreptului intern;
- (i) subiecții testării în condiții reale și-au dat consimțământul în cunoștință de cauză în conformitate cu articolul 61 sau, în cazul aplicării legii, în cazul în care solicitarea consimțământului în cunoștință de cauză ar împiedica testarea sistemului de IA, testarea în sine și rezultatul testării în condiții reale nu au niciun efect negativ asupra subiecților, iar datele cu caracter personal ale acestora se șterg după efectuarea testării;

- (j) testarea în condiții reale este supravegheată efectiv de furnizor sau de potențialul furnizor, precum și de implementatori sau de potențialii implementatori prin intermediul unor persoane care sunt calificate corespunzător în domeniul relevant și care au capacitatea, formarea și autoritatea necesare pentru a-și îndeplini sarcinile;
 - (k) previziunile, recomandările sau deciziile sistemului de IA pot fi efectiv inversate și ignorate.
- (5) Orice subiecți ai testării în condiții reale sau reprezentanții lor desemnați legal, după caz, se pot retrage din testare în orice moment, fără vreun prejudiciu și fără a trebui să prezinte vreo justificare, prin revocarea consimțământului lor în cunoștință de cauză și pot solicita ștergerea imediată și permanentă a datelor lor cu caracter personal. Retragera consimțământului în cunoștință de cauză nu afectează activitățile deja desfășurate.
- (6) În conformitate cu articolul 75, statele membre conferă autorităților lor de supraveghere a pieței competența de a solicita informații furnizorilor și potențialilor furnizori, de a efectua inspecții neanunțate la distanță sau la fața locului și de a efectua verificări privind efectuarea testării în condiții reale și a sistemelor de IA cu grad ridicat de risc conexe. Autoritățile de supraveghere a pieței fac uz de aceste competențe pentru a asigura o dezvoltare în condiții de siguranță a testării în condiții reale.

- (7) Orice incident grav identificat în cursul testării în condiții reale se raportează autorității naționale de supraveghere a pieței în conformitate cu articolul 73. Furnizorul sau potențialul furnizor adoptă măsuri imediate de atenuare sau, în caz contrar, suspendă testarea în condiții reale până când are loc o astfel de atenuare sau îi pune capăt în alt mod. Furnizorul sau potențialul furnizor instituie o procedură pentru rechemarea promptă a sistemului de IA în cazul unei astfel de încetări a testării în condiții reale.
- (8) Furnizorii sau potențialii furnizori informează autoritatea națională de supraveghere a pieței din statul membru în care se efectuează testarea în condiții reale cu privire la suspendarea sau încetarea testării în condiții reale și cu privire la rezultatele finale.
- (9) Furnizorul sau potențialul furnizor este responsabil, în temeiul dreptului aplicabil al Uniunii și al dreptului intern în materie de răspundere, pentru orice prejudiciu cauzat în cursul testării în condiții reale pe care o efectuează.

Articolul 61

Consimțământul în cunoștință de cauză la participarea la testarea în condiții reale în afara spațiilor de testare în materie de reglementare în domeniul IA

- (1) În scopul testării în condiții reale în conformitate cu articolul 60, consimțământul în cunoștință de cauză acordat în mod liber se obține de la subiecții testării înainte de participarea lor la o astfel de testare și după ce au fost informați în mod corespunzător cu informații concise, clare, relevante și inteligibile cu privire la:
- (a) natura și obiectivele testării în condiții reale și posibilele inconveniente care ar putea fi legate de participarea lor;
 - (b) condițiile în care se desfășoară testarea în condiții reale, inclusiv durata preconizată a participării subiectului sau a subiecților;
 - (c) drepturile lor și garanțiile cu privire la participarea lor, în special dreptul lor de a refuza să participe la testarea în condiții reale și dreptul de a se retrage din aceasta în orice moment, fără angajarea vreunui prejudiciu și fără a fi nevoiți să prezinte vreo justificare;
 - (d) modalitățile de solicitare a inversării sau a ignorării previziunilor, recomandărilor sau deciziilor sistemului de IA;
 - (e) numărul unic de identificare la nivelul întregii Uniuni al testării în condiții reale în conformitate cu articolul 60 alineatul (4) litera (c) și datele de contact ale furnizorului sau ale reprezentantului său legal de la care se pot obține informații suplimentare.

- (2) Consimțământul în cunoștință de cauză se datează și se documentează, iar o copie se înmânează subiecților testării sau reprezentanților lor legali.

Articolul 62

Măsuri pentru furnizori și implementatori, în special IMM-uri, inclusiv întreprinderi nou-înființate

- (1) Statele membre întreprind următoarele acțiuni:
- (a) oferă IMM-urilor, inclusiv întreprinderilor nou-înființate, care au un sediu social sau o sucursală în Uniune, acces prioritar la spațiile de testare în materie de reglementare în domeniul IA, în măsura în care îndeplinesc condițiile de eligibilitate și criteriile de selecție; accesul prioritar nu împiedică accesul altor IMM-uri, inclusiv întreprinderi nou-înființate, altele decât cele menționate la prezentul alineat, la spațiile de testare în materie de reglementare în domeniul IA, cu condiția ca acestea să îndeplinească de asemenea condițiile de eligibilitate și criteriile de selecție;
 - (b) organizează activități specifice de sensibilizare și formare cu privire la aplicarea prezentului regulament, adaptate la nevoile IMM-urilor, inclusiv ale întreprinderilor nou-înființate, ale implementatorilor și, după caz, ale autorităților publice locale;
 - (c) utilizează canalele specifice existente și, după caz, stabilesc altele noi pentru comunicarea cu IMM-urile, inclusiv cu întreprinderile nou-înființate, cu implementatorii, cu alți inovatori și, după caz, cu autoritățile publice locale, pentru a oferi consiliere și a răspunde la întrebări cu privire la aplicarea prezentului regulament, inclusiv în ceea ce privește participarea la spațiile de testare în materie de reglementare în domeniul IA;

- (d) facilitează participarea IMM-urilor și a altor părți interesate relevante la procesul de dezvoltare a standardizării.
- (2) Interesele și nevoile specifice ale IMM-urilor furnizoare, inclusiv ale întreprinderilor nou-înființate, sunt luate în considerare la stabilirea taxelor pentru evaluarea conformității în temeiul articolului 43, taxele respective fiind reduse proporțional cu dimensiunile acestora, cu dimensiunea pieței și cu alți indicatori relevanți.
- (3) Oficiul pentru IA întreprinde următoarele acțiuni:
- (a) furnizează modele standardizate pentru domeniile vizate de prezentul regulament, astfel cum specifică Consiliul IA în cererea sa;
 - (b) dezvoltă și menține o platformă unică de informare care să ofere informații ușor de utilizat în legătură cu prezentul regulament pentru toți operatorii din întreaga Uniune;
 - (c) organizează campanii de comunicare adecvate pentru a sensibiliza publicul cu privire la obligațiile care decurg din prezentul regulament;
 - (d) evaluează și promovează convergența bunelor practici în procedurile de achiziții publice în ceea ce privește sistemele de IA.

Articolul 63

Derogări pentru operatori specifici

- (1) Microîntreprinderile în sensul Recomandării 2003/361/CE pot respecta anumite elemente ale sistemului de management al calității prevăzut la articolul 17 din prezentul regulament într-un mod simplificat, cu condiția să nu aibă întreprinderi partenere sau întreprinderi afiliate în sensul recomandării respective. În acest scop, Comisia elaborează orientări privind elementele sistemului de management al calității care pot fi respectate într-un mod simplificat, având în vedere nevoile microîntreprinderilor, fără a afecta nivelul de protecție sau necesitatea respectării cerințelor în ceea ce privește sistemele de IA cu grad ridicat de risc.
- (2) Alineatul (1) de la prezentul articol nu se interpretează ca o exceptare a operatorilor respectivi de la îndeplinirea oricăror alte cerințe sau obligații prevăzute în prezentul regulament, inclusiv cele stabilite la articolele 9, 10, 11, 12, 13, 14, 15, 72 și 73.

Capitolul VII

Guvernanța

SECȚIUNEA 1

GUVERNANȚA LA NIVELUL UNIUNII

Articolul 64

Oficiul pentru IA

- (1) Comisia dezvoltă cunoștințele de specialitate și capabilitățile Uniunii în domeniul IA prin intermediul Oficiului pentru IA.
- (2) Statele membre facilitează sarcinile încredințate Oficiului pentru IA, astfel cum sunt reflectate în prezentul regulament.

Articolul 65

Instituirea și structura Consiliului european pentru inteligența artificială

- (1) Se instituie un Consiliu european pentru inteligența artificială (denumit în continuare „Consiliul IA”).

- (2) Consiliul IA este alcătuit dintr-un reprezentant pentru fiecare stat membru. Autoritatea Europeană pentru Protecția Datelor participă ca observator. Oficiul pentru IA participă, de asemenea, la reuniunile Consiliului IA fără a lua parte la vot. De la caz la caz, Consiliul IA poate invita la reuniuni și alte autorități, organisme sau experți de la nivel național și de la nivelul Uniunii, în cazul în care chestiunile discutate prezintă relevanță pentru acestea.
- (3) Fiecare reprezentant este desemnat de statul său membru pentru o perioadă de trei ani, care poate fi reînnoită o singură dată.
- (4) Statele membre se asigură că reprezentanții lor în Consiliul IA:
- (a) dețin competențele și prerogativele relevante în statul lor membru, astfel încât să contribuie în mod activ la îndeplinirea sarcinilor Consiliului IA menționate la articolul 66;
 - (b) sunt desemnați ca punct unic de contact pentru Consiliul IA și, după caz, ținând seama de nevoile statelor membre, ca punct unic de contact pentru părțile interesate;
 - (c) sunt împuterniciți să faciliteze coerența și coordonarea între autoritățile naționale competente din statul lor membru în ceea ce privește punerea în aplicare a prezentului regulament, inclusiv prin colectarea de date și informații relevante în scopul îndeplinirii sarcinilor care le revin în cadrul Consiliului IA.
- (5) Reprezentanții desemnați ai statelor membre adoptă regulamentul de procedură al Consiliului IA cu o majoritate de două treimi. Regulamentul de procedură stabilește, în special, procedurile pentru procesul de selecție, durata mandatului și specificațiile sarcinilor președintelui, modalitățile detaliate pentru votare și organizarea activităților Consiliului IA și a celor ale subgroupurilor acestuia.

(6) Consiliul IA instituie două subgrupuri permanente pentru a oferi o platformă de cooperare și de schimb între autoritățile de supraveghere a pieței și autoritățile de notificare cu privire la aspecte legate de supravegherea pieței și, respectiv, de organisme notificate.

Subgrupul permanent pentru supravegherea pieței ar trebui să acționeze în calitate de grup de cooperare administrativă (ADCO) pentru prezentul regulament în sensul articolului 30 din Regulamentul (UE) 2019/1020.

Consiliul IA poate înființa alte subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice. După caz, reprezentanții Forumului consultativ menționat la articolul 67 pot fi invitați la astfel de subgrupuri sau la reuniuni specifice ale subgrupurilor respective în calitate de observatori.

(7) Consiliul IA este organizat și funcționează astfel încât să garanteze obiectivitatea și imparțialitatea activităților sale.

(8) Consiliul IA este prezidat de către unul dintre reprezentanții statelor membre.

Oficiul pentru IA asigură secretariatul pentru Consiliul IA, convoacă reuniunile la cererea președintelui și pregătește ordinea de zi în conformitate cu sarcinile care îi revin Consiliului IA în temeiul prezentului regulament și al regulamentului său de procedură.

Articolul 66

Sarcinile Consiliului IA

Consiliul IA oferă consiliere și asistență Comisiei și statelor membre pentru a facilita aplicarea coerentă și eficace a prezentului regulament. În acest scop, Consiliul IA poate, în special:

- (a) să contribuie la coordonarea între autoritățile naționale competente responsabile cu aplicarea prezentului regulament și, în cooperare cu autoritățile de supraveghere a pieței în cauză și sub rezerva acordului acestora, să sprijine activitățile comune ale autorităților de supraveghere a pieței menționate la articolul 74 alineatul (11);
- (b) să colecteze și să disemineze în rândul statelor membre cunoștințe de specialitate tehnice și în materie de reglementare și de bune practici;
- (c) să ofere consiliere privind punerea în aplicare a prezentului regulament, în special în ceea ce privește aplicarea normelor privind modelele de IA de uz general;
- (d) să contribuie la armonizarea practicilor administrative din statele membre, inclusiv în ceea ce privește derogarea de la procedurile de evaluare a conformității menționate la articolul 46, funcționarea spațiilor de testare în materie de reglementare în domeniul IA și testarea în condiții reale menționate la articolele 57, 59 și 60;

- (e) la cererea Comisiei sau din proprie inițiativă, să emită recomandări și avize scrise cu privire la orice aspecte relevante legate de punerea în aplicare a prezentului regulament și de aplicarea coerentă și efectivă a acestuia, inclusiv:
- (i) elaborarea și aplicarea codurilor de conduită și a codurilor de bune practici în temeiul prezentului regulament, precum și al orientărilor Comisiei;
 - (ii) evaluarea și revizuirea prezentului regulament în temeiul articolului 112, inclusiv în ceea ce privește rapoartele privind incidentele grave menționate la articolul 73 și funcționarea bazei de date a UE menționate la articolul 71, pregătirea actelor delegate sau de punere în aplicare și în ceea ce privește posibilele alinieri ale prezentului regulament la legislația de armonizare a Uniunii enumerată în anexa I;
 - (iii) specificațiile tehnice sau standardele existente referitoare la cerințele prevăzute în capitolul III secțiunea 2;
 - (iv) utilizarea standardelor armonizate sau a specificațiilor comune menționate la articolele 40 și 41;
 - (v) tendințele în aspecte precum competitivitatea europeană la nivel mondial în domeniul IA, adoptarea IA în Uniune și dezvoltarea competențelor digitale;
 - (vi) tendințele în ceea ce privește tipologia în continuă evoluție a lanțurilor valorice ale IA, în special referitor la implicațiile rezultate în ceea ce privește responsabilitatea;

- (vii) eventuala necesitate de modificare a anexei III în conformitate cu articolul 7 și privind eventuala necesitate de a revizui articolul 5 în temeiul articolului 112, ținând seama de dovezile relevante disponibile și de cele mai recente evoluții tehnologice;
- (f) să sprijine Comisia în promovarea alfabetizării în domeniul IA, a acțiunilor de sensibilizare și de înțelegere în rândul publicului a beneficiilor, riscurilor, garanțiilor și drepturilor și obligațiilor legate de utilizarea sistemelor de IA;
- (g) să faciliteze elaborarea unor criterii comune și a unei înțelegeri comune între operatorii de pe piață și autoritățile competente a conceptelor relevante prevăzute în prezentul regulament, inclusiv prin contribuirea la elaborarea de criterii de referință;
- (h) să coopereze, după caz, cu alte instituții, organe, oficii și agenții relevante ale Uniunii, precum și cu grupuri de experți și rețelele relevante ale Uniunii, în special în domeniul siguranței produselor, al securității cibernetice, al concurenței, al serviciilor digitale și media, al serviciilor financiare, al protecției consumatorilor, al protecției datelor și a drepturilor fundamentale;
- (i) să contribuie la cooperarea eficace cu autoritățile competente din țările terțe și cu organizațiile internaționale;
- (j) să sprijine autoritățile naționale competente și Comisia în dezvoltarea cunoștințelor de specialitate organizaționale și tehnice necesare pentru punerea în aplicare a prezentului regulament, inclusiv prin contribuirea la evaluarea nevoilor de formare pentru personalul statelor membre implicat în punerea în aplicare a prezentului regulament;

- (k) să sprijine Oficiul pentru IA în acordarea de asistență autorităților naționale competente pentru crearea și dezvoltarea de spații de testare în materie de reglementare în domeniul IA și să faciliteze cooperarea și schimbul de informații între spațiile de testare în materie de reglementare în domeniul IA;
- (l) să contribuie la elaborarea documentelor de orientare și să ofere consiliere relevantă cu privire la aceasta;
- (m) să consilieze Comisia în legătură cu chestiuni internaționale privind IA;
- (n) să furnizeze Comisiei avize cu privire la alertele calificate referitoare la modelele de IA de uz general;
- (o) să primească opinii din partea statelor membre cu privire la alertele calificate referitoare la modelele de IA de uz general și la experiențele și practicile naționale privind monitorizarea sistemelor de IA și aplicarea normelor referitoare la acestea, îndeosebi sistemele care integrează modelele de IA de uz general.

Articolul 67

Forumul consultativ

- (1) Se instituie un forum consultativ pentru a furniza cunoștințe de specialitate tehnice Consiliului IA și Comisiei și pentru a le consilia, precum și pentru a contribui la sarcinile care le revin în temeiul prezentului regulament.
- (2) Componenta Forumului consultativ reprezintă o selecție echilibrată a părților interesate, inclusiv a sectorului, a întreprinderilor nou-înființate, a IMM-urilor, a societății civile și a mediului academic. Componenta Forumului consultativ este echilibrată între interesele comerciale și necomerciale și, în cadrul categoriei intereselor comerciale, în ceea ce privește IMM-urile și alte întreprinderi.

- (3) Comisia numește membrii Forumului consultativ, în conformitate cu criteriile stabilite la alineatul (2), din rândul părților interesate cu cunoștințe de specialitate recunoscute în domeniul IA.
- (4) Mandatul membrilor Forumului consultativ este de doi ani și poate fi prelungit cu cel mult patru ani.
- (5) Agenția pentru Drepturi Fundamentale a Uniunii Europene, ENISA, Comitetul European de Standardizare (CEN), Comitetul European de Standardizare în Electrotehnică (CENELEC) și Institutul European de Standardizare în Telecomunicații (ETSI) sunt membri permanenți ai Forumului consultativ.
- (6) Forumul consultativ își stabilește regulamentul de procedură. Acesta alege doi copreședinți dintre membrii săi, în conformitate cu criteriile stabilite la alineatul (2). Mandatul copreședinților este de doi ani, reînnoibil o singură dată.
- (7) Forumul consultativ organizează reuniuni de cel puțin două ori pe an. Forumul consultativ poate invita experți și alte părți interesate la reuniunile sale.
- (8) Forumul consultativ poate elabora avize, recomandări și contribuții scrise la cererea Consiliului IA sau a Comisiei.
- (9) Forumul consultativ poate institui subgrupuri permanente sau temporare, după caz, în scopul examinării unor chestiuni specifice legate de obiectivele prezentului regulament.
- (10) Forumul consultativ întocmește un raport anual privind activitățile sale. Raportul respectiv este pus la dispoziția publicului.

Articolul 68

Grupul științific de experți independenți

- (1) Comisia, prin intermediul unui act de punere în aplicare, adoptă dispoziții privind instituirea unui grup științific de experți independenți (denumit în continuare „grupul științific”) menit să sprijine activitățile de aplicare a legii în temeiul prezentului regulament. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).
- (2) Grupul științific este alcătuit din experți independenți selectați de Comisie pe baza cunoștințelor de specialitate științifice sau tehnice la zi în domeniul IA, necesare pentru îndeplinirea sarcinilor prevăzute la alineatul (3), și este în măsură să demonstreze îndeplinirea tuturor condițiilor următoare:
 - (a) să dispună de cunoștințe de specialitate și competențe specifice și cunoștințe de specialitate științifice și tehnice în domeniul IA;
 - (b) să fie independent față de orice furnizor de sisteme de IA sau de modele de IA de uz general;
 - (c) să aibă capacitatea de a desfășura activități cu diligență, acuratețe și obiectivitate.

Comisia, în consultare cu Consiliul IA, stabilește numărul de experți din grup în funcție de necesități și asigură o reprezentare geografică și de gen echitabilă.

- (3) Grupul științific consiliază și sprijină Oficiul pentru IA, în special în ceea ce privește următoarele sarcini:
- (a) sprijinirea punerii în aplicare și a respectării prezentului regulament, în ceea ce privește modelele și sistemele de IA de uz general, îndeosebi prin:
 - (i) alertarea Oficiului pentru IA cu privire la posibile riscuri sistemice la nivelul Uniunii prezentate de modele de IA de uz general, în conformitate cu articolul 90;
 - (ii) contribuirea la dezvoltarea instrumentelor și metodologiilor de evaluare a capabilităților modelelor și sistemelor de IA de uz general, inclusiv prin valori de referință;
 - (iii) furnizarea de consiliere cu privire la clasificarea sistemelor de IA de uz general cu risc sistemic;
 - (iv) furnizarea de consiliere cu privire la clasificarea diverselor modele și sisteme de IA de uz general;
 - (v) contribuirea la dezvoltarea de instrumente și modele;
 - (b) sprijinirea activității autorităților de supraveghere a pieței, la cererea acestora;
 - (c) sprijinirea activităților transfrontaliere în materie de supraveghere a pieței menționate la articolul 74 alineatul (11), fără a aduce atingere competențelor autorităților de supraveghere a pieței;

- (d) sprijinirea Oficiului pentru IA în îndeplinirea sarcinilor sale în contextul procedurii de salvagardare a Uniunii în temeiul articolului 81.
- (4) Experții din cadrul grupului științific își îndeplinesc sarcinile cu imparțialitate și obiectivitate și asigură confidențialitatea informațiilor și a datelor obținute în cursul îndeplinirii sarcinilor și activităților lor. Aceștia nu solicită și nici nu acceptă instrucțiuni de la nicio persoană atunci când își exercită atribuțiile în temeiul alineatului (3). Fiecare expert întocmește o declarație de interese, care este pusă la dispoziția publicului. Oficiul pentru IA instituie sisteme și proceduri pentru a gestiona în mod activ și pentru a preveni potențialele conflicte de interese.
- (5) Actul de punere în aplicare menționat la alineatul (1) include dispoziții privind condițiile, procedurile și modalitățile detaliate pentru emiterea de alerte de către grupul științific și membrii săi și pentru solicitarea de către aceștia de asistență din partea Oficiului pentru IA în îndeplinirea sarcinilor grupului științific.

Articolul 69

Accesul statelor membre la grupul de experți

- (1) Statele membre pot apela la experți din cadrul grupului științific pentru sprijinirea activităților lor de aplicare a legii în temeiul prezentului regulament.

- (2) Statele membre pot fi obligate să plătească taxe pentru consilierea și sprijinul furnizate de experți. Structura și nivelul taxelor, precum și amplexarea și structura costurilor recuperabile sunt stabilite în actul de punere în aplicare menționat la articolul 68 alineatul (1), ținând seama de obiectivele punerii în aplicare adecvate a prezentului regulament, de raportul cost-eficacitate și de necesitatea de a asigura pentru toate statele membre accesul efectiv la experți.
- (3) Comisia facilitează accesul în timp util al statelor membre la experți, după caz, și se asigură că combinarea activităților de sprijin desfășurate de structurile de sprijin pentru testarea IA ale Uniunii în temeiul articolului 84 și de experți în temeiul prezentului articol este organizată în mod eficient și oferă cea mai bună valoare adăugată posibilă.

SECȚIUNEA 2

AUTORITĂȚILE NAȚIONALE COMPETENTE

Articolul 70

Desemnarea autorităților naționale competente și a punctelor unice de contact

- (1) Fiecare stat membru stabilește sau desemnează drept autorități naționale competente cel puțin o autoritate de notificare și cel puțin o autoritate de supraveghere a pieței în sensul prezentului regulament. Respectivăle autorități naționale competente își exercită competențele în mod independent, imparțial și fără prejudecăți, astfel încât să garanteze obiectivitatea activităților și sarcinilor lor și să asigure punerea în aplicare a prezentului regulament. Membrii acestor autorități se abțin de la orice act incompatibil cu atribuțiile lor. Cu condiția ca aceste principii să fie respectate, astfel de activități și sarcini pot fi efectuate de una sau mai multe autorități desemnate, în conformitate cu nevoile organizaționale ale statului membru.
- (2) Statele membre îi comunică Comisiei identitatea autorităților de notificare și a autorităților de supraveghere a pieței și sarcinile acestor autorități, precum și orice modificări ulterioare ale acestora. Până la ... [12 luni de la data intrării în vigoare a prezentului regulament], statele membre pun la dispoziția publicului informații cu privire la modul în care pot fi contactate autoritățile competente și punctele unice de contact, prin mijloace de comunicare electronică. Statele membre desemnează o autoritate de supraveghere a pieței care să acționeze ca punct unic de contact pentru prezentul regulament și îi notifică Comisiei identitatea punctului unic de contact. Comisia pune la dispoziția publicului o listă a punctelor unice de contact.

- (3) Statele membre se asigură că autoritățile lor naționale competente dispun de resurse tehnice, financiare și umane adecvate și de infrastructură pentru a-și îndeplini cu eficacitate sarcinile care le revin în temeiul prezentului regulament. În special, autoritățile naționale competente dispun în permanență de un personal suficient ale cărui competențe și cunoștințe de specialitate includ o înțelegere aprofundată a tehnologiilor din domeniul IA, a datelor și a prelucrării de date, a protecției datelor cu caracter personal, a securității cibernetice, a drepturilor fundamentale, a riscurilor în materie de sănătate și siguranță, precum și cunoașterea standardelor și a cerințelor legale existente. Statele membre evaluează și, dacă este necesar, actualizează anual competențele și resursele necesare menționate la prezentul alineat.
- (4) Autoritățile naționale competente iau măsuri corespunzătoare pentru a asigura un nivel de securitate cibernetică adecvat.
- (5) Atunci când își îndeplinesc sarcinile, autoritățile naționale competente acționează în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.
- (6) Până la ... [un an de la data intrării în vigoare a prezentului regulament] și, ulterior, la fiecare doi ani, statele membre îi prezintă Comisiei un raport privind situația resurselor financiare și umane ale autorităților naționale competente, împreună cu o evaluare a adecvării acestora. Comisia transmite aceste informații Consiliului IA pentru a fi discutate și pentru a formula eventuale recomandări.
- (7) Comisia facilitează schimbul de experiență între autoritățile naționale competente.

- (8) Autoritățile naționale competente pot oferi orientări și consiliere cu privire la punerea în aplicare a prezentului regulament, îndeosebi IMM-urilor, inclusiv întreprinderilor nou-înființate, luând în considerare orientările și consilierea furnizate de Consiliul IA și de Comisie, după caz. Ori de câte ori autoritățile naționale competente intenționează să ofere orientări și consiliere cu privire la un sistem de IA în domenii reglementate de alte acte legislative ale Uniunii, autoritățile naționale competente în temeiul actelor legislative respective ale Uniunii sunt consultate, după caz.
- (9) Atunci când instituțiile, organele, oficiile sau agențiile Uniunii intră în domeniul de aplicare al prezentului regulament, Autoritatea Europeană pentru Protecția Datelor acționează ca autoritate competentă pentru supravegherea lor.

Capitolul VIII

Baza de date a UE pentru sisteme de ia cu grad ridicat de risc

Articolul 71

Baza de date a UE pentru sisteme de IA cu grad ridicat de risc enumerate în anexa III

- (1) Comisia, în colaborare cu statele membre, creează și întreține o bază de date a UE care conține informațiile menționate la alineatele (2) și (3) de la prezentul articol privind sistemele de IA cu grad ridicat de risc menționate la articolul 6 alineatul (2) care sunt înregistrate în conformitate cu articolele 49 și 60 și sistemele de IA care nu sunt considerate ca având un grad ridicat de risc în temeiul articolului 6 alineatul (3) și care sunt înregistrate în conformitate cu articolul 6 alineatul (4) și cu articolul 49. Atunci când stabilește specificațiile funcționale ale respectivei baze de date, Comisia consultă experții relevanți, iar atunci când actualizează specificațiile funcționale ale respectivei baze de date, Comisia consultă Consiliul IA.

- (2) Datele enumerate în secțiunile A și B din anexa VIII se introduc în baza de date a UE de către furnizor sau, după caz, de către reprezentantul autorizat.
- (3) Datele enumerate în secțiunea C din anexa VIII se introduc în baza de date a UE de către implementatorul care este o autoritate publică, o agenție sau un organ ori care acționează în numele acestora, în conformitate cu articolul 49 alineatele (3) și (4).
- (4) Cu excepția secțiunii menționate la articolul 49 alineatul (4) și la articolul 60 alineatul (4) litera (c), informațiile conținute în baza de date a UE înregistrate în conformitate cu articolul 49 sunt accesibile și puse la dispoziția publicului într-un mod ușor de utilizat. Informațiile ar trebui să fie ușor de navigat și prelucrabile automat. Informațiile înregistrate în conformitate cu articolul 60 sunt accesibile numai autorităților de supraveghere a pieței și Comisiei, cu excepția cazului în care potențialul furnizor sau furnizorul și-a dat consimțământul pentru ca aceste informații să fie puse și la dispoziția publicului.
- (5) Baza de date a UE conține date cu caracter personal numai în măsura în care acest lucru este necesar pentru colectarea și prelucrarea informațiilor în conformitate cu prezentul regulament. Aceste informații includ numele și datele de contact ale persoanelor fizice responsabile cu înregistrarea sistemului și care au autoritatea legală de a-l reprezenta pe furnizor sau pe implementator, după caz.
- (6) Comisia este operatorul bazei de date a UE. Aceasta pune la dispoziția furnizorilor, a potențialilor furnizori și a implementatorilor sprijin tehnic și administrativ adecvat. Baza de date a UE respectă cerințele de accesibilitate aplicabile.

Capitolul IX

Monitorizarea ulterioară introducerii pe piață, schimbul de informații și supravegherea pieței

SECȚIUNEA 1

MONITORIZAREA ULTERIOARĂ INTRODUCERII PE PIAȚĂ

Articolul 72

Monitorizarea ulterioară introducerii pe piață de către furnizori și planul de monitorizare ulterioară introducerii pe piață pentru sistemele de IA cu grad ridicat de risc

- (1) Furnizorii instituie și documentează un sistem de monitorizare ulterioară introducerii pe piață într-un mod care să fie proporțional cu natura tehnologiilor din domeniul IA și cu riscurile sistemului de IA cu grad ridicat de risc.
- (2) Sistemul de monitorizare ulterioară introducerii pe piață colectează, documentează și analizează în mod activ și sistematic datele relevante care pot fi furnizate de implementatori sau pot fi colectate din alte surse cu privire la performanța sistemelor de IA cu grad ridicat de risc pe toată durata lor de viață și care permit furnizorului să evalueze conformitatea continuă a sistemelor de IA cu cerințele prevăzute în capitolul III secțiunea 2. După caz, monitorizarea ulterioară introducerii pe piață include o analiză a interacțiunii cu alte sisteme de IA. Această obligație nu acoperă datele operaționale sensibile ale implementatorilor care sunt autorități de aplicare a legii.

- (3) Sistemul de monitorizare ulterioară introducerii pe piață se bazează pe un plan de monitorizare ulterioară introducerii pe piață. Planul de monitorizare ulterioară introducerii pe piață face parte din documentația tehnică menționată în anexa IV. Comisia adoptă un act de punere în aplicare prin care stabilește dispoziții detaliate de stabilire a unui model de plan de monitorizare ulterioară introducerii pe piață și a listei elementelor care trebuie incluse în plan până la ... [18 luni de la data intrării în vigoare a prezentului regulament]. Actul de punere în aplicare respectiv se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).
- (4) Pentru sistemele de IA cu grad ridicat de risc reglementate de actele legislative de armonizare ale Uniunii menționate în secțiunea A din anexa I, în cazul în care un sistem și un plan de monitorizare ulterioară introducerii pe piață sunt deja instituite în temeiul legislației respective, pentru a asigura coerența, a evita suprapunerile și a reduce la minimum sarcinile suplimentare, furnizorii au posibilitatea de a integra, după caz, elementele necesare descrise la alineatele (1), (2) și (3), utilizând modelul menționat la alineatul (3), în sistemele și planurile deja existente în temeiul legislației respective, cu condiția ca astfel să atingă un nivel de protecție echivalent.

Primul paragraf de la prezentul alineat se aplică, de asemenea, sistemelor de IA cu grad ridicat de risc menționate la punctul 5 din anexa III introduse pe piață sau puse în funcțiune de instituții financiare care fac obiectul unor cerințe privind guvernanta lor internă, măsurile sau procesele lor interne în temeiul dreptului Uniunii din domeniul serviciilor financiare.

SECȚIUNEA 2

SCHIMBUL DE INFORMAȚII PRIVIND INCIDENTELE GRAVE

Articolul 73

Raportarea incidentelor grave

- (1) Furnizorii de sisteme de IA cu grad ridicat de risc introduse pe piața Uniunii raportează orice incident grav autorităților de supraveghere a pieței din statele membre în care s-a produs incidentul respectiv.
- (2) Raportul menționat la alineatul (1) se efectuează imediat după ce furnizorul a stabilit o legătură de cauzalitate între sistemul de IA și incidentul grav sau probabilitatea rezonabilă a unei astfel de legături și, în orice caz, nu mai târziu de 15 zile de la data la care furnizorul sau, după caz, implementatorul a luat cunoștință de incidentul grav.

Termenul pentru raportarea menționată la primul paragraf ține seama de gravitatea incidentului grav.

- (3) În pofida alineatului (2) de la prezentul articol, în cazul unei încălcări pe scară largă sau al unui incident grav, astfel cum sunt definite la articolul 3 punctul 49 litera (b), raportul menționat la alineatul (1) de la prezentul articol se furnizează imediat și în termen de cel mult două zile de la data la care furnizorul sau, după caz, implementatorul a luat cunoștință de incidentul respectiv.

- (4) În pofida alineatului (2), în caz de deces al unei persoane, raportul se pune la dispoziție imediat după ce furnizorul sau implementatorul a stabilit sau de îndată ce suspectează o legătură de cauzalitate între sistemul de IA cu grad ridicat de risc și incidentul grav, dar nu mai târziu de 10 zile de la data la care furnizorul sau, după caz, implementatorul a luat cunoștință de incidentul grav.
- (5) Dacă este necesar pentru a asigura raportarea în timp util, furnizorul sau, după caz, implementatorul poate prezenta un raport inițial care este incomplet, urmat de un raport complet.
- (6) În urma raportării unui incident grav în temeiul alineatului (1), furnizorul efectuează, fără întârziere, investigațiile necesare cu privire la incidentul grav și la sistemul de IA în cauză. Acest lucru include o evaluare a riscurilor incidentului și măsuri corective.

În cursul investigațiilor menționate la primul paragraf, furnizorul cooperează cu autoritățile competente și, după caz, cu organismul notificat în cauză și nu efectuează nicio investigație care presupune modificarea sistemului de IA în cauză într-un mod care poate afecta orice evaluare ulterioară a cauzelor incidentului, înainte de a informa autoritățile competente în legătură cu o astfel de acțiune.

- (7) La primirea unei notificări referitoare la un incident grav menționat la articolul 3 punctul 49 litera (c), autoritatea relevantă de supraveghere a pieței informează autoritățile sau organismele publice naționale menționate la articolul 77 alineatul (1). Comisia elaborează orientări specifice pentru a facilita respectarea obligațiilor prevăzute la alineatul (1) de la prezentul articol. Orientările respective se emit până la ... [12 luni de la data intrării în vigoare a prezentului regulament] și se evaluează periodic.

- (8) Autoritatea de supraveghere a pieței ia măsurile corespunzătoare, astfel cum se prevede la articolul 19 din Regulamentul (UE) 2019/1020, în termen de șapte de zile de la data la care a primit notificarea menționată la alineatul (1) de la prezentul articol și urmează procedurile de notificare prevăzute în respectivul regulament.
- (9) În cazul sistemelor de IA cu grad ridicat de risc menționate în anexa III care sunt introduse pe piață sau puse în funcțiune de furnizori care fac obiectul unor instrumente legislative ale Uniunii care prevăd obligații de raportare echivalente cu cele prevăzute în prezentul regulament, notificarea incidentelor grave se limitează la cele menționate la articolul 3 punctul 49 litera (c).
- (10) În cazul sistemelor de IA cu grad ridicat de risc care sunt componente de siguranță ale unor dispozitive sau sunt ele însele dispozitive care fac obiectul Regulamentelor (UE) 2017/745 și (UE) 2017/746, notificarea incidentelor grave se limitează la cele menționate la articolul 3 punctul 49 litera (c) din prezentul regulament și se efectuează către autoritatea națională competentă aleasă în acest scop de statele membre în care s-a produs incidentul respectiv.
- (11) Autoritățile naționale competente îi notifică imediat Comisiei orice incident grav, indiferent dacă au luat sau nu măsuri cu privire la acesta, în conformitate cu articolul 20 din Regulamentul (UE) 2019/1020.

SECȚIUNEA 3

APLICAREA LEGII

Articolul 74

Supravegherea pieței și controlul sistemelor de IA pe piața Uniunii

- (1) Regulamentul (UE) 2019/1020 se aplică sistemelor de IA care intră sub incidența prezentului regulament. În scopul asigurării efective a respectării prezentului regulament:
 - (a) orice trimitere la un operator economic în temeiul Regulamentului (UE) 2019/1020 se interpretează ca incluzând toți operatorii identificați la articolul 2 alineatul (1) din prezentul regulament;
 - (b) orice trimitere la un produs în temeiul Regulamentului (UE) 2019/1020 se interpretează ca incluzând toate sistemele de IA care intră în domeniul de aplicare al prezentului regulament.
- (2) Ca parte a obligațiilor lor de raportare în temeiul articolului 34 alineatul (4) din Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței raportează anual Comisiei și autorităților naționale de concurență relevante toate informațiile identificate în cursul activităților de supraveghere a pieței care ar putea prezenta un potențial interes pentru aplicarea dreptului Uniunii privind normele în materie de concurență. De asemenea, acestea raportează anual Comisiei despre utilizarea practicilor interzise care a avut loc în anul respectiv și despre măsurile luate.
- (3) În cazul sistemelor de IA cu grad ridicat de risc legate de produse reglementate de actele legislative de armonizare ale Uniunii enumerate în secțiunea A din anexa I, autoritatea de supraveghere a pieței în sensul prezentului regulament este autoritatea responsabilă cu activitățile de supraveghere a pieței desemnată în temeiul respectivelor acte legislative.

Prin derogare de la primul paragraf și în circumstanțe corespunzătoare, statele membre pot desemna o altă autoritate relevantă care să acționeze în calitate de autoritate de supraveghere a pieței, cu condiția ca acestea să asigure coordonarea cu autoritățile sectoriale relevante de supraveghere a pieței responsabile cu aplicarea legislației de armonizare a Uniunii enumerate în anexa I.

- (4) Procedurile menționate la articolele 79-83 din prezentul regulament nu se aplică sistemelor de IA legate de produse reglementate de actele legislative de armonizare ale Uniunii enumerate în secțiunea A din anexa I, atunci când respectivele acte juridice prevăd deja proceduri care asigură un nivel de protecție echivalent și care au același obiectiv. În astfel de cazuri, se aplică în schimb procedurile sectoriale relevante.
- (5) Fără a aduce atingere competențelor autorităților de supraveghere a pieței în temeiul articolului 14 din Regulamentul (UE) 2019/1020, în scopul aplicării efective a prezentului regulament, autoritățile de supraveghere a pieței pot exercita de la distanță competențele menționate la articolul 14 alineatul (4) literele (d) și (j) din respectivul regulament, după caz.
- (6) Pentru sistemele de IA cu grad ridicat de risc introduse pe piață, puse în funcțiune sau utilizate de instituțiile financiare reglementate de dreptul Uniunii din domeniul serviciilor financiare, autoritatea de supraveghere a pieței în sensul prezentului regulament este autoritatea națională relevantă responsabilă cu supravegherea financiară a instituțiilor respective în temeiul legislației respective, în măsura în care introducerea pe piață, punerea în funcțiune sau utilizarea sistemului de IA este în legătură directă cu furnizarea serviciilor financiare respective.

- (7) Prin derogare de la alineatul (6), în circumstanțe justificate și cu condiția asigurării coordonării, o altă autoritate relevantă poate fi identificată de statul membru drept autoritate de supraveghere a pieței în sensul prezentului regulament.

Autoritățile naționale de supraveghere a pieței care supraveghează instituțiile de credit reglementate în temeiul Directivei 2013/36/UE, care participă la mecanismul unic de supraveghere instituit prin Regulamentul (UE) nr. 1024/2013, ar trebui să raporteze fără întârziere Băncii Centrale Europene orice informație identificată în cursul activităților lor de supraveghere a pieței care ar putea prezenta un interes potențial pentru sarcinile de supraveghere prudențială ale Băncii Centrale Europene, astfel cum se specifică în regulamentul respectiv.

- (8) Pentru sistemele de IA cu grad ridicat de risc enumerate la punctul 1 din anexa III la prezentul regulament, în măsura în care sistemele sunt utilizate în scopul aplicării legii, al gestionării frontierelor și al respectării justiției și democrației, și pentru sistemele de IA cu grad ridicat de risc enumerate la punctele 6, 7 și 8 din anexa III la prezentul regulament, statele membre desemnează drept autorități de supraveghere a pieței în sensul prezentului regulament fie autoritățile competente de supraveghere a protecției datelor în temeiul Regulamentului (UE) 2016/679 sau al Directivei (UE) 2016/680, fie orice alte autorități desemnate în temeiul aceluiași condiții prevăzute la articolele 41-44 din Directiva (UE) 2016/680. Activitățile de supraveghere a pieței nu afectează în niciun fel independența autorităților judiciare și nici nu interferează în alt mod cu activitățile acestora atunci când acționează în exercițiul funcției lor judiciare.

- (9) În cazul în care instituții, organe, oficii sau agenții ale Uniunii intră în domeniul de aplicare al prezentului regulament, Autoritatea Europeană pentru Protecția Datelor acționează în calitate de autoritate de supraveghere a pieței pentru acestea, cu excepția cazurilor în care Curtea de Justiție a Uniunii Europene acționează în exercițiul funcției sale judiciare.
- (10) Statele membre facilitează coordonarea dintre autoritățile de supraveghere a pieței desemnate în temeiul prezentului regulament și alte autorități sau organisme naționale relevante care supraveghează aplicarea actelor legislative de armonizare ale Uniunii enumerate în anexa I sau în alte acte legislative ale Uniunii care ar putea fi relevante pentru sistemele de IA cu grad ridicat de risc menționate în anexa III.
- (11) Autoritățile de supraveghere a pieței și Comisia sunt în măsură să propună activități comune, inclusiv investigații comune, care să fie efectuate fie de autoritățile de supraveghere a pieței, fie de autoritățile de supraveghere a pieței în colaborare cu Comisia și care au scopul de a promova conformitatea, de a identifica cazurile de neconformitate, de a sensibiliza sau de a oferi orientări în legătură cu prezentul regulament în ceea ce privește anumite categorii de sisteme de IA cu grad ridicat de risc despre care se constată că prezintă un risc grav în două sau mai multe state membre, în conformitate cu articolul 9 din Regulamentul (UE) 2019/1020. Oficiul pentru IA oferă sprijin în materie de coordonare pentru investigațiile comune.

- (12) Fără a aduce atingere competențelor prevăzute în Regulamentul (UE) 2019/1020 și dacă este relevant și limitat la ceea ce este necesar pentru a-și îndeplini sarcinile, furnizorii acordă acces deplin autorităților de supraveghere a pieței la documentație, precum și la seturile de date de antrenament, de validare și de testare utilizate pentru dezvoltarea sistemelor de IA cu grad ridicat de risc, inclusiv, după caz și sub rezerva unor garanții de securitate, prin interfețe de programare a aplicațiilor (IPA) sau prin alte mijloace și instrumente tehnice relevante care permit accesul de la distanță.
- (13) Autorităților de supraveghere a pieței li se acordă acces la codul sursă al sistemului de IA cu grad ridicat de risc pe baza unei cereri motivate și numai atunci când sunt îndeplinite ambele condiții următoare:
- (a) accesul la codul sursă este necesar pentru a evalua conformitatea unui sistem de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul III secțiunea 2; și
 - (b) procedurile de testare sau de audit și verificările bazate pe datele și documentația furnizate de furnizor au fost epuizate sau s-au dovedit insuficiente.
- (14) Orice informații sau documentație obținute de autoritățile de supraveghere a pieței în temeiul prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 75

Asistența reciprocă, supravegherea pieței și controlul sistemelor de IA de uz general

- (1) În cazul în care un sistem de IA se bazează pe un model de IA de uz general, iar modelul și sistemul sunt dezvoltate de același furnizor, Oficiul pentru IA are competența de a monitoriza și de a supraveghea conformitatea respectivului sistem de IA cu obligațiile impuse în temeiul prezentului regulament. Pentru a își îndeplini sarcinile de monitorizare și supraveghere, Oficiul pentru IA are toate competențele unei autorități de supraveghere a pieței prevăzute în prezenta secțiune și în Regulamentul (UE) 2019/1020.
- (2) În cazul în care au motive suficiente să considere că sisteme de IA de uz general care pot fi utilizate direct de către implementatori pentru cel puțin un scop clasificat ca prezentând un grad ridicat de risc în temeiul prezentului regulament nu respectă cerințele prevăzute în prezentul regulament, autoritățile relevante de supraveghere a pieței cooperează cu Oficiul pentru IA pentru a efectua evaluări ale conformității și informează în consecință Consiliul IA și alte autorități de supraveghere a pieței.

- (3) Dacă o autoritate de supraveghere a pieței nu este în măsură să își încheie investigația privind sistemul de IA cu grad ridicat de risc din cauza incapacității sale de a accesa anumite informații legate de modelul de IA de uz general, în pofida faptului că a depus toate eforturile adecvate pentru a obține informațiile respective, aceasta poate transmite Oficiului pentru IA o cerere motivată prin care accesul la respectivele informații este impus. În acest caz, Oficiul pentru IA îi furnizează autorității solicitante fără întârziere și, în orice caz, în termen de 30 de zile toate informațiile pe care Oficiul pentru IA le consideră relevante pentru a stabili dacă un sistem de IA cu grad ridicat de risc este neconform. Autoritățile de supraveghere a pieței garantează confidențialitatea informațiilor pe care le obțin în conformitate cu articolul 78 din prezentul regulament. Procedura prevăzută în capitolul VI din Regulamentul (UE) 2019/1020 se aplică *mutatis mutandis*.

Articolul 76

Supravegherea testării în condiții reale de către autoritățile de supraveghere a pieței

- (1) Autoritățile de supraveghere a pieței dețin competențele și prerogativele necesare pentru a se asigura că testarea în condiții reale este conformă cu prezentul regulament.
- (2) În cazul în care se efectuează testarea în condiții reale pentru sisteme de IA care sunt supravegheate într-un spațiu de testare în materie de reglementare în domeniul IA în temeiul articolului 58, autoritățile de supraveghere a pieței verifică conformitatea cu articolul 60 ca parte a rolului lor de supraveghere pentru spațiul de testare în materie de reglementare în domeniul IA. Autoritățile respective pot permite, după caz, ca testarea în condiții reale să fie efectuată de furnizor sau de potențialul furnizor, prin derogare de la condițiile prevăzute la articolul 60 alineatul (4) literele (f) și (g).

- (3) În cazul în care o autoritate de supraveghere a pieței a fost informată de către potențialul furnizor, de către furnizor sau de către orice parte terță despre un incident grav sau are alte motive pentru a considera că nu sunt îndeplinite condițiile prevăzute la articolele 60 și 61, aceasta poate lua oricare dintre următoarele decizii pe teritoriul său, după caz:
- (a) suspendarea sau încetarea testării în condiții reale;
 - (b) solicitarea furnizorului sau a potențialului furnizor și a implementatorului sau a potențialului implementator să modifice orice aspect al testării în condiții reale.
- (4) În cazul în care o autoritate de supraveghere a pieței a luat o decizie menționată la alineatul (3) de la prezentul articol sau a emis o obiecție în sensul articolului 60 alineatul (4) litera (b), decizia sau obiecția indică motivele care stau la baza acesteia, precum și modul în care furnizorul sau potențialul furnizor poate contesta decizia sau obiecția.
- (5) După caz, dacă o autoritate de supraveghere a pieței a luat o decizie menționată la alineatul (3), aceasta comunică motivele care stau la baza deciziei respective autorităților de supraveghere a pieței din celelalte state membre în care sistemul de IA a fost testat în conformitate cu planul de testare.

Articolul 77

Competențele autorităților care protejează drepturile fundamentale

- (1) Autoritățile sau organismele publice naționale care supraveghează sau asigură respectarea obligațiilor în temeiul dreptului Uniunii care protejează drepturile fundamentale, inclusiv dreptul la nediscriminare, în ceea ce privește utilizarea sistemelor de IA cu grad ridicat de risc menționate în anexa III au competența de a solicita și de a accesa orice documentație creată sau păstrată în temeiul prezentului regulament într-un limbaj și un format accesibil, atunci când accesul la documentația respectivă este necesar pentru îndeplinirea cu eficacitate a mandatelor lor, în limitele jurisdicției lor. Autoritatea sau organismul public competent informează autoritatea de supraveghere a pieței din statul membru în cauză cu privire la orice astfel de cerere.
- (2) Până la ... [trei luni de la data intrării în vigoare a prezentului regulament], fiecare stat membru identifică autoritățile sau organismele publice menționate la alineatul (1) și pune o listă a acestora la dispoziția publicului. Statele membre îi notifică lista Comisiei și celorlalte state membre și o mențin la zi.
- (3) În cazul în care documentația menționată la alineatul (1) este insuficientă pentru a stabili dacă a avut loc sau nu o încălcare a obligațiilor în temeiul dreptului Uniunii care protejează drepturile fundamentale, autoritatea sau organismul public menționat la alineatul (1) poate adresa autorității de supraveghere a pieței o cerere motivată de organizare a testării sistemului de IA cu grad ridicat de risc prin mijloace tehnice. Autoritatea de supraveghere a pieței organizează testarea implicând îndeaproape autoritatea sau organismul public solicitant, într-un termen rezonabil de la primirea cererii.

- (4) Toate informațiile și documentele obținute de autoritățile sau organismele publice naționale menționate la alineatul (1) de la prezentul articol în temeiul dispozițiilor prezentului articol sunt tratate în conformitate cu obligațiile de confidențialitate prevăzute la articolul 78.

Articolul 78
Confidențialitate

- (1) Comisia, autoritățile de supraveghere a pieței și organismele notificate, precum și orice altă persoană fizică sau juridică implicată în aplicarea prezentului regulament respectă, în conformitate cu dreptul Uniunii sau cu dreptul intern, confidențialitatea informațiilor și a datelor obținute în îndeplinirea sarcinilor și a activităților lor într-un mod care să protejeze, în special:
- (a) drepturile de proprietate intelectuală și informațiile comerciale confidențiale sau secretele comerciale ale unei persoane fizice sau juridice, inclusiv codul sursă, cu excepția cazurilor menționate la articolul 5 din Directiva (UE) 2016/943 a Parlamentului European și a Consiliului⁵⁷;
 - (b) punerea efectivă în aplicare a prezentului regulament, în special în scopul inspecțiilor, investigațiilor și auditurilor;
 - (c) interesele de securitate publică și națională;
 - (d) desfășurarea procedurilor penale sau administrative;

⁵⁷ Directiva (UE) 2016/943 a Parlamentului European și a Consiliului din 8 iunie 2016 privind protecția know-how-ului și a informațiilor de afaceri nedivulgate (secrete comerciale) împotriva dobândirii, utilizării și divulgării ilegale (JO L 157, 15.6.2016, p. 1).

- (e) informațiile clasificate în temeiul dreptului Uniunii sau al dreptului intern.
- (2) Autoritățile implicate în aplicarea prezentului regulament în temeiul alineatului (1) solicită numai datele care sunt strict necesare pentru evaluarea riscului prezentat de sistemele de IA și pentru exercitarea competențelor lor în conformitate cu prezentul regulament și cu Regulamentul (UE) 2019/1020. Acestea instituie măsuri de securitate cibernetică corespunzătoare și eficiente pentru a proteja securitatea și confidențialitatea informațiilor și a datelor obținute și șterg datele colectate de îndată ce acestea nu mai sunt necesare în scopul pentru care au fost obținute, în conformitate cu dreptul Uniunii sau dreptul intern aplicabil.
- (3) Fără a aduce atingere alineatelor (1) și (2), informațiile care au făcut obiectul unui schimb în condiții de confidențialitate între autoritățile naționale competente și între autoritățile naționale competente și Comisie nu se divulgă fără consultarea prealabilă a autorității naționale competente emitente și a implementatorului atunci când sistemele de IA cu grad ridicat de risc menționate la punctul 1, 6 sau 7 din anexa III sunt utilizate de autoritățile de aplicare a legii, de control la frontiere, de imigrație sau de azil și atunci când o astfel de divulgare ar pune în pericol interese de siguranță publică și de securitate națională. Acest schimb de informații nu acoperă datele operaționale sensibile legate de activitățile autorităților de aplicare a legii, de control la frontiere, de imigrație sau de azil.

În cazul în care autoritățile de aplicare a legii, de imigrație sau de azil sunt furnizori de sisteme de IA cu grad ridicat de risc menționate la punctul 1, 6 sau 7 din anexa III, documentația tehnică menționată în anexa IV rămâne la sediul autorităților respective. Autoritățile respective se asigură că autoritățile de supraveghere a pieței menționate la articolul 74 alineatele (8) și (9), după caz, pot, la cerere, să acceseze imediat documentația sau să obțină o copie a acesteia. Numai personalului autorității de supraveghere a pieței care deține nivelul corespunzător de autorizare de securitate i se permite accesul la documentația respectivă sau la orice copie a acesteia.

- (4) Alineatele (1), (2) și (3) nu aduc atingere drepturilor și obligațiilor care revin Comisiei, statelor membre și autorităților relevante ale acestora, precum și celor care revin organismelor notificate cu privire la schimbul de informații și difuzarea avertizărilor, inclusiv în contextul cooperării transfrontaliere, și nu aduc atingere nici obligațiilor părților în cauză de a furniza informații în temeiul dreptului penal al statelor membre.
- (5) Comisia și statele membre pot face schimb, atunci când este necesar și în conformitate cu dispozițiile relevante din acordurile internaționale și comerciale, de informații confidențiale cu autoritățile de reglementare din țări terțe cu care au încheiat acorduri de confidențialitate bilaterale sau multilaterale care garantează un nivel adecvat de confidențialitate.

Articolul 79

Procedura la nivel național aplicabilă sistemelor de IA care prezintă un risc

- (1) Prin sisteme de IA care prezintă un risc se înțelege un „produs care prezintă un risc”, în sensul definiției de la articolul 3 punctul 19 din Regulamentul (UE) 2019/1020, în măsura în care prezintă riscuri pentru sănătatea sau siguranța ori pentru drepturile fundamentale ale persoanelor.

- (2) În cazul în care autoritatea de supraveghere a pieței dintr-un stat membru are suficiente motive să considere că un sistem de IA prezintă un risc astfel cum se menționează la alineatul (1) de la prezentul articol, aceasta efectuează o evaluare a sistemului de IA în cauză din punctul de vedere al conformității sale cu toate cerințele și obligațiile prevăzute în prezentul regulament. Se acordă o atenție deosebită sistemelor de IA care prezintă un risc pentru grupurile vulnerabile. Atunci când sunt identificate riscuri pentru drepturile fundamentale, autoritatea de supraveghere a pieței informează și autoritățile sau organismele publice naționale relevante menționate la articolul 77 alineatul (1) și cooperează pe deplin cu acestea. Operatorii relevanți cooperează, după caz, cu autoritatea de supraveghere a pieței și cu celelalte autorități sau organisme publice naționale menționate la articolul 77 alineatul (1).

În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței sau, după caz, autoritatea de supraveghere a pieței în cooperare cu autoritatea publică națională menționată la articolul 77 alineatul (1) constată că sistemul de IA nu respectă cerințele și obligațiile prevăzute în prezentul regulament, aceasta solicită fără întârzieri nejustificate operatorului relevant să ia toate măsurile corective adecvate pentru a asigura conformitatea sistemului de IA, pentru a retrage sistemul de IA de pe piață sau pentru a-l rechema într-un termen pe care autoritatea de supraveghere a pieței îl poate indica și, în orice caz, nu mai târziu de 15 zile lucrătoare sau astfel cum se prevede în actele legislative de armonizare relevante ale Uniunii.

Autoritățile de supraveghere a pieței informează organismul notificat relevant în consecință. Articolul 18 din Regulamentul (UE) 2019/1020 se aplică măsurilor menționate la al doilea paragraf de la prezentul alineat.

- (3) În cazul în care autoritatea de supraveghere a pieței consideră că neconformitatea nu se limitează la teritoriul său național, aceasta informează fără întârzieri nejustificate Comisia și celelalte state membre cu privire la rezultatele evaluării și la măsurile pe care i le-a impus operatorului.
- (4) Operatorul se asigură că sunt luate toate măsurile corective adecvate pentru toate sistemele de IA în cauză pe care acesta le-a pus la dispoziție pe piața Uniunii.
- (5) În cazul în care operatorul unui sistem de IA nu ia măsurile corective adecvate în termenul menționat la alineatul (2), autoritatea de supraveghere a pieței ia toate măsurile provizorii corespunzătoare pentru a interzice sau a restricționa punerea la dispoziție a sistemului de IA pe piața sa națională sau punerea acestuia în funcțiune, pentru a retrage produsul sau sistemul de IA de sine stătător de pe piața respectivă ori pentru a-l rechema. Autoritatea respectivă notifică fără întârzieri nejustificate Comisiei și celorlalte state membre măsurile respective.
- (6) Notificarea menționată la alineatul (5) include toate detaliile disponibile, în special informațiile necesare pentru a identifica sistemul de IA neconform, originea sistemului de IA și lanțul de aprovizionare, natura neconformității invocate și riscul implicat, natura și durata măsurilor naționale luate, precum și argumentele prezentate de operatorul relevant. În special, autoritățile de supraveghere a pieței indică dacă neconformitatea se datorează unuia sau mai multora dintre următoarele motive:
- (a) nerespectarea interdicției privind practicile în domeniul IA menționate la articolul 5;
 - (b) nerespectarea de către sistemul de IA cu grad ridicat de risc a cerințelor prevăzute în capitolul III secțiunea 2;

- (c) existența unor deficiențe în ceea ce privește standardele armonizate sau specificațiile comune menționate la articolele 40 și 41 care conferă o prezumție de conformitate;
 - (d) nerespectarea articolului 50.
- (7) Autoritățile de supraveghere a pieței, altele decât autoritatea de supraveghere a pieței din statul membru care a inițiat procedura, informează fără întârzieri nejustificate Comisia și celelalte state membre cu privire la toate măsurile adoptate și la toate informațiile suplimentare deținute referitoare la neconformitatea sistemului de IA în cauză și, în cazul unui dezacord cu măsura națională notificată, cu privire la obiecțiile lor.
- (8) În cazul în care, în termen de trei luni de la primirea notificării menționate la alineatul (5) de la prezentul articol, nicio autoritate de supraveghere a pieței a niciunui stat membru și nici Comisia nu ridică vreo obiecție cu privire la o măsură provizorie luată de o autoritate de supraveghere a pieței a unui alt stat membru, măsura respectivă este considerată justificată. Acest lucru nu aduce atingere drepturilor procedurale ale operatorului în cauză în conformitate cu articolul 18 din Regulamentul (UE) 2019/1020. Termenul de trei luni menționat la prezentul alineat se reduce la 30 de zile în cazul nerespectării interdicției privind practicile în domeniul IA menționate la articolul 5 din prezentul regulament.
- (9) Autoritățile de supraveghere a pieței se asigură că se iau măsuri restrictive adecvate în ceea ce privește produsul sau sistemul de IA în cauză, cum ar fi retragerea fără întârzieri nejustificate a produsului sau a sistemului de IA de pe piețele lor.

Articolul 80

Procedura aplicabilă sistemelor de IA clasificate de furnizor ca neprezentând un grad ridicat de risc în aplicarea anexei III

- (1) În cazul în care o autoritate de supraveghere a pieței are motive suficiente să considere că un sistem de IA clasificat de furnizor ca neprezentând un grad ridicat de risc în conformitate cu articolul 6 alineatul (3) prezintă, de fapt, un grad ridicat de risc, autoritatea de supraveghere a pieței efectuează o evaluare a sistemului de IA în cauză în ceea ce privește clasificarea sa ca sistem de IA cu grad ridicat de risc, pe baza condițiilor prevăzute la articolul 6 alineatul (3) și în orientările Comisiei.
- (2) În cazul în care, pe parcursul evaluării respective, autoritatea de supraveghere a pieței constată că sistemul de IA în cauză prezintă un grad ridicat de risc, aceasta solicită fără întârzieri nejustificate furnizorului relevant să ia toate măsurile necesare pentru a asigura conformitatea sistemului de IA cu cerințele și obligațiile prevăzute în prezentul regulament, precum și să ia măsuri corective adecvate într-un termen pe care autoritatea de supraveghere a pieței îl poate indica.
- (3) În cazul în care autoritatea de supraveghere a pieței consideră că utilizarea sistemului de IA în cauză nu se limitează la teritoriul său național, aceasta informează fără întârzieri nejustificate Comisia și celelalte state membre cu privire la rezultatele evaluării și la măsurile pe care i le-a impus furnizorului.

- (4) Furnizorul se asigură că se iau toate măsurile necesare pentru a asigura conformitatea sistemului de IA cu cerințele și obligațiile prevăzute în prezentul regulament. În cazul în care furnizorul unui sistem de IA în cauză nu asigură conformitatea sistemului de IA cu respectivele cerințe și obligații în termenul menționat la alineatul (2) de la prezentul articol, furnizorului i se aplică amenzi în conformitate cu articolul 99.
- (5) Furnizorul se asigură că sunt întreprinse toate măsurile corective adecvate pentru toate sistemele de IA în cauză pe care acesta le-a pus la dispoziție pe piața Uniunii.
- (6) Dacă furnizorul sistemului de IA în cauză nu ia măsurile corective adecvate în termenul menționat la alineatul (2) de la prezentul articol, se aplică articolul 79 alineatele (5)-(9).
- (7) Dacă, în cursul evaluării respective în temeiul alineatului (1) de la prezentul articol, autoritatea de supraveghere a pieței stabilește că sistemul de IA a fost clasificat greșit de furnizor ca neprezentând un grad ridicat de risc pentru a eluda aplicarea cerințelor de la capitolul III secțiunea 2, furnizorului i se aplică amenzi în conformitate cu articolul 99.
- (8) În exercitarea competenței lor de monitorizare a aplicării prezentului articol și în conformitate cu articolul 11 din Regulamentul (UE) 2019/1020, autoritățile de supraveghere a pieței pot efectua verificări adecvate, ținând seama în special de informațiile stocate în baza de date a UE menționată la articolul 71 din prezentul regulament.

Articolul 81

Procedura de salvagardare a Uniunii

- (1) Dacă, în termen de trei luni de la primirea notificării menționate la articolul 79 alineatul (5) sau în termen de 30 de zile în cazul nerespectării interdicției privind practicile în domeniul IA menționate la articolul 5, se ridică obiecții de către autoritatea de supraveghere a pieței a unui stat membru împotriva unei măsuri luate de altă autoritate de supraveghere a pieței sau în cazul în care Comisia consideră că măsura este contrară dreptului Uniunii, Comisia inițiază fără întârzieri nejustificate consultări cu autoritatea de supraveghere a pieței a statului membru relevant și cu operatorul sau operatorii și evaluează măsura națională. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura națională este justificată sau nu în termen de șase luni ori, în cazul nerespectării interdicției privind practicile în domeniul IA menționate la articolul 5, în termen de 60 de zile de la notificarea menționată la articolul 79 alineatul (5) și notifică această decizie autorității de supraveghere a pieței a statului membru în cauză. Comisia informează, de asemenea, toate celelalte autorități de supraveghere a pieței cu privire la decizia sa.
- (2) În cazul în care Comisia consideră că măsura luată de statul membru în cauză este justificată, toate statele membre se asigură că iau măsuri restrictive adecvate în ceea ce privește sistemul de IA în cauză, cum ar fi impunerea retragerii fără întârzieri nejustificate a sistemului de IA de pe piața lor, și informează Comisia în consecință. În cazul în care Comisia consideră că măsura națională este nejustificată, statul membru în cauză retrage măsura și informează Comisia în consecință.

- (3) Atunci când măsura națională este considerată justificată, iar neconformitatea sistemului de IA este atribuită unor deficiențe ale standardelor armonizate sau ale specificațiilor comune menționate la articolele 40 și 41 din prezentul regulament, Comisia aplică procedura prevăzută la articolul 11 din Regulamentul (UE) nr. 1025/2012.

Articolul 82

Sisteme de IA conforme care prezintă un risc

- (1) Dacă, în urma efectuării unei evaluări în temeiul articolului 79, după consultarea autorității publice naționale relevante menționate la articolul 77 alineatul (1), autoritatea de supraveghere a pieței dintr-un stat membru constată că, deși un sistem de IA cu grad ridicat de risc este în conformitate cu prezentul regulament, acesta prezintă totuși un risc pentru sănătatea sau siguranța persoanelor, pentru drepturile fundamentale sau pentru alte aspecte legate de protecția interesului public, autoritatea de supraveghere a pieței respectivă impune operatorului relevant să ia toate măsurile corespunzătoare pentru a se asigura că sistemul de IA în cauză, atunci când este introdus pe piață sau pus în funcțiune, nu mai prezintă riscul respectiv fără întârzieri nejustificate, într-un termen pe care aceasta îl poate indica.
- (2) Furnizorul sau alt operator relevant se asigură că sunt luate măsuri corective cu privire la toate sistemele de IA în cauză pe care le-a pus la dispoziție pe piața Uniunii, în termenul prevăzut de autoritatea de supraveghere a pieței din statul membru menționat la alineatul (1).

- (3) Statele membre informează imediat Comisia și celelalte state membre cu privire la o constatare în temeiul alineatului (1). Informațiile includ toate detaliile disponibile, în special datele necesare pentru identificarea sistemului de IA în cauză, originea și a lanțul de aprovizionare aferent acestuia, natura riscului implicat, precum și natura și durata măsurilor naționale luate.
- (4) Comisia inițiază fără întârzieri nejustificate consultări cu statele membre în cauză și cu operatorii relevanți și evaluează măsurile naționale luate. Pe baza rezultatelor evaluării respective, Comisia decide dacă măsura este justificată și, după caz, propune alte măsuri adecvate.
- (5) Comisia comunică imediat decizia sa statelor membre în cauză și operatorilor relevanți. Aceasta informează, de asemenea, celelalte state membre.

Articolul 83

Neconformitatea formală

- (1) Autoritatea de supraveghere a pieței dintr-un stat membru solicită operatorului relevant să pună capăt neconformității în cauză, într-un termen pe care aceasta îl poate indica, atunci când constată una dintre situațiile următoare:
 - (a) marcajul CE a fost aplicat cu încălcarea articolului 48;
 - (b) marcajul CE nu a fost aplicat;
 - (c) declarația de conformitate UE menționată la articolul 47 nu a fost întocmită;

- (d) declarația de conformitate UE menționată la articolul 47 nu a fost întocmită corect;
 - (e) nu a fost efectuată înregistrarea în baza de date a UE menționată la articolul 71;
 - (f) după caz, nu a fost numit un reprezentant autorizat;
 - (g) documentația tehnică nu este disponibilă.
- (2) În cazul în care neconformitatea menționată la alineatul (1) persistă, autoritatea de supraveghere a pieței din statul membru în cauză ia măsuri corespunzătoare și proporționale pentru a restricționa sau a interzice punerea la dispoziție pe piață a sistemului de IA cu grad ridicat de risc sau pentru a se asigura că acesta este rechemat sau retras de pe piață fără întârziere.

Articolul 84

Structurile de sprijin pentru testarea IA ale Uniunii

- (1) Comisia desemnează una sau mai multe structuri de sprijin pentru testarea IA ale Uniunii pentru a îndeplini sarcinile enumerate la articolul 21 alineatul (6) din Regulamentul (UE) 2019/1020 în domeniul IA.
- (2) Fără a aduce atingere sarcinilor menționate la alineatul (1), structurile de sprijin pentru testarea IA ale Uniunii furnizează, de asemenea, consiliere tehnică sau științifică independentă la cererea Consiliului IA, a Comisiei sau a autorităților de supraveghere a pieței.

SECȚIUNEA 4

CĂI DE ATAC

Articolul 85

Dreptul de a depune o plângere la o autoritate de supraveghere a pieței

Fără a aduce atingere altor căi de atac administrative sau judiciare, orice persoană fizică sau juridică care are motive să considere că a avut loc o încălcare a dispozițiilor prezentului regulament poate depune plângeri la autoritatea de supraveghere a pieței relevantă.

În conformitate cu Regulamentul (UE) 2019/1020, astfel de plângeri sunt luate în considerare în scopul desfășurării activităților de supraveghere a pieței și sunt tratate în conformitate cu procedurile specifice stabilite în acest scop de autoritățile de supraveghere a pieței.

Articolul 86

Dreptul la explicarea luării deciziilor individuale

- (1) Orice persoană afectată care face obiectul unei decizii care este luată de implementator pe baza rezultatelor unui sistem de IA cu grad ridicat de risc enumerat în anexa III, cu excepția sistemelor enumerate la punctul 2 din aceasta, și care produce efecte juridice sau o afectează pe persoana respectivă în mod similar într-un grad semnificativ de o manieră pe care o consideră a avea un impact negativ asupra sănătății, siguranței sau drepturilor sale fundamentale are dreptul de a solicita implementatorului explicații clare și semnificative cu privire la rolul sistemului de IA în procedura decizională și la principalele elemente ale deciziei luate.

- (2) Alineatul (1) nu se aplică utilizării sistemelor de IA pentru care excepțiile sau restricțiile de la obligația prevăzută la alineatul respectiv decurg din dreptul Uniunii sau din dreptul intern în conformitate cu dreptul Uniunii.
- (3) Prezentul articol se aplică numai în măsura în care dreptul menționat la alineatul (1) nu este deja prevăzut în dreptul Uniunii.

Articolul 87

Raportarea încălcărilor și protecția persoanelor care efectuează raportarea

În ceea ce privește raportarea încălcărilor prezentului regulament și protecția persoanelor care raportează astfel de încălcări se aplică Directiva (UE) 2019/1937.

SECȚIUNEA 5

SUPRAVEGHEREA, INVESTIGAREA, APLICAREA LEGII ȘI MONITORIZAREA ÎN CEEA CE PRIVEȘTE FURNIZORII DE MODELE DE IA DE UZ GENERAL

Articolul 88

Executarea obligațiilor furnizorilor de modele de IA de uz general

- (1) Comisia are competențe exclusive de a supraveghea și de a asigura respectarea capitolului V, ținând seama de garanțiile procedurale în temeiul articolului 94. Comisia încredințează Oficiului pentru IA punerea în aplicare a acestor sarcini, fără a aduce atingere competențelor de organizare ale Comisiei și repartizării competențelor între statele membre și Uniune pe baza tratatelor.

- (2) Fără a aduce atingere articolului 75 alineatul (3), autoritățile de supraveghere a pieței îi pot solicita Comisiei să își exercite competențele prevăzute în prezenta secțiune, în cazul în care acest lucru este necesar și proporțional pentru a sprijini îndeplinirea sarcinilor care le revin în temeiul prezentului regulament.

Articolul 89

Măsurile de monitorizare

- (1) În scopul îndeplinirii sarcinilor care îi sunt atribuite în temeiul prezentei secțiuni, Oficiul pentru IA poate lua măsurile necesare pentru a monitoriza punerea în aplicare și respectarea efectivă a prezentului regulament de către furnizorii de modele de IA de uz general, inclusiv respectarea de către aceștia a codurilor de bune practici aprobate.
- (2) Furnizorii din aval au dreptul de a depune o plângere privind încălcarea prezentului regulament. O plângere trebuie să fie motivată corespunzător și să indice cel puțin:
- (a) punctul de contact al furnizorului modelului de IA de uz general în cauză;
 - (b) o descriere a faptelor relevante, a dispozițiilor vizate ale prezentului regulament și a motivului pentru care furnizorul din aval consideră că furnizorul modelului de IA de uz general în cauză a încălcat prezentul regulament;
 - (c) orice alte informații pe care furnizorul din aval care a transmis cererea le consideră relevante, inclusiv, după caz, informații colectate din proprie inițiativă.

Articolul 90

Alerte privind riscurile sistemice transmise de grupul științific

- (1) Grupul științific poate transmite o alertă calificată către Oficiul pentru IA în cazul în care are motive să suspecteze că:
 - (a) un model de IA de uz general prezintă un risc identificabil concret la nivelul Uniunii; sau
 - (b) un model de IA de uz general îndeplinește condițiile menționate la articolul 51.
- (2) În urma unei astfel de alerte calificate, Comisia, prin intermediul Oficiului pentru IA și după ce a informat Consiliul IA, poate exercita competențele prevăzute în prezenta secțiune în scopul analizării chestiunii. Oficiul pentru IA informează Consiliul IA cu privire la orice măsură în conformitate cu articolele 91-94.
- (3) O alertă calificată trebuie să fie motivată corespunzător și să indice cel puțin:
 - (a) punctul de contact al furnizorului modelului de IA de uz general cu risc sistemic în cauză;
 - (b) o descriere a faptelor relevante și a motivelor care stau la baza alertei transmise de grupul științific;
 - (c) orice alte informații pe care grupul științific le consideră relevante, inclusiv, după caz, informații colectate din proprie inițiativă.

Articolul 91

Competența de a solicita documente și informații

- (1) Comisia poate solicita furnizorului modelului de IA de uz general în cauză să furnizeze documentația întocmită de furnizor în conformitate cu articolele 53 și 55 sau orice informații suplimentare care sunt necesare în scopul evaluării conformității furnizorului cu prezentul regulament.
- (2) Înainte de trimiterea cererii de informații, Oficiul pentru IA poate iniția un dialog structurat cu furnizorul modelului de IA de uz general.
- (3) La cererea justificată în mod corespunzător a grupului științific, Comisia poate emite o cerere de informații adresată unui furnizor al unui model de IA de uz general, în cazul în care accesul la informații este necesar și proporțional pentru îndeplinirea sarcinilor grupului științific în temeiul articolului 68 alineatul (2).
- (4) Cererea de informații precizează temeiul juridic și scopul cererii, specifică informațiile solicitate, stabilește termenul în care acestea trebuie furnizate și indică amenziile prevăzute la articolul 101 pentru furnizarea de informații incorecte, incomplete sau înșelătoare.

- (5) Furnizorul modelului de IA de uz general în cauză sau reprezentantul acestuia furnizează informațiile solicitate. În cazul persoanelor juridice, al societăților sau firmelor ori în cazul în care furnizorul nu are personalitate juridică, persoanele autorizate să le reprezinte în temeiul legii sau al statutului lor furnizează informațiile solicitate în numele furnizorului modelului de IA de uz general în cauză. Juriștii autorizați corespunzător să acționeze în acest sens pot furniza informațiile în numele clienților lor. Clienții rămân totuși pe deplin răspunzători în situația în care informațiile furnizate sunt incomplete, incorecte sau înșelătoare.

Articolul 92

Competența de a efectua evaluări

- (1) Oficiul pentru IA, după consultarea Consiliului IA, poate efectua evaluări ale modelului de IA de uz general în cauză:
- (a) pentru a evalua respectarea de către furnizor a obligațiilor care îi revin în temeiul prezentului regulament, în cazul în care informațiile colectate în temeiul articolului 91 sunt insuficiente; sau
 - (b) pentru a investiga riscurile sistemice la nivelul Uniunii ale modelelor de IA de uz general cu risc sistemic, în special în urma unei alerte calificate a grupului științific în conformitate cu articolul 90 alineatul (1) litera (a).
- (2) Comisia poate decide să numească experți independenți care să efectueze evaluări în numele său, inclusiv din cadrul grupului științific instituit în temeiul articolului 68. Experții independenți numiți pentru această sarcină îndeplinesc criteriile menționate la articolul 68 alineatul (2).

- (3) În sensul alineatului (1), Comisia poate solicita accesul la modelul de IA de uz general în cauză prin intermediul API sau al altor mijloace și instrumente tehnice adecvate, inclusiv codul sursă.
- (4) Cererea de acces menționează temeiul juridic, scopul și motivele cererii și stabilește termenul în care trebuie acordat accesul, precum și amenzile prevăzute la articolul 101 pentru neacordarea accesului.
- (5) Furnizorul modelului de IA de uz general în cauză sau reprezentantul acestuia furnizează informațiile solicitate. În cazul persoanelor juridice, societăților sau firmelor ori în cazul în care furnizorul nu are personalitate juridică, persoanele autorizate să îl reprezinte în temeiul legii sau al statutului său furnizează accesul solicitat în numele furnizorului modelului de IA de uz general în cauză.
- (6) Comisia adoptă acte de punere în aplicare care stabilesc modalitățile detaliate și condițiile evaluărilor, inclusiv modalitățile detaliate de implicare a experților independenți, precum și procedura de selecție a acestora. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).
- (7) Înainte de a solicita accesul la modelul de IA de uz general în cauză, Oficiul pentru IA poate iniția un dialog structurat cu furnizorul modelului de IA de uz general, pentru a colecta mai multe informații cu privire la testarea internă a modelului, la garanțiile interne pentru prevenirea riscurilor sistemice și la alte proceduri și măsuri interne pe care furnizorul le-a instituit pentru a atenua astfel de riscuri.

Articolul 93
Competența de a solicita măsuri

- (1) În cazul în care este necesar și adecvat, Comisia le poate solicita furnizorilor:
 - (a) să ia măsuri adecvate pentru a respecta obligațiile prevăzute la articolele 53 și 54;
 - (b) să pună în aplicare măsuri de atenuare, în cazul în care evaluarea efectuată în conformitate cu articolul 92 a dat naștere unei preocupări serioase și întemeiate cu privire la un risc sistemic la nivelul Uniunii;
 - (c) să restricționeze punerea la dispoziție pe piață a modelului, să îl retragă sau să îl recheme.
- (2) Înainte de a solicita o măsură, Oficiul pentru IA poate iniția un dialog structurat cu furnizorul modelului de IA de uz general.
- (3) În cazul în care, în cursul dialogului structurat menționat la alineatul (2), furnizorul modelului de IA de uz general cu risc sistemic își asumă angajamente de a pune în aplicare măsuri de atenuare a unui risc sistemic la nivelul Uniunii, Comisia poate, prin intermediul unei decizii, să confere respectivelor angajamente caracter obligatoriu și să declare că nu există alte motive pentru a acționa.

Articolul 94

Drepturile procedurale ale operatorilor economici ai modelului de IA de uz general

Articolul 18 din Regulamentul (UE) 2019/1020 se aplică *mutatis mutandis* furnizorilor modelului de IA de uz general, fără a aduce atingere drepturilor procedurale mai specifice prevăzute în prezentul regulament.

Capitolul X

Coduri de conduită și orientări

Articolul 95

Coduri de conduită pentru aplicarea voluntară a cerințelor specifice

- (1) Oficiul pentru IA și statele membre încurajează și facilitează elaborarea de coduri de conduită, inclusiv mecanisme de guvernare conexe, menite să promoveze aplicarea voluntară în cazul altor sisteme de IA decât sistemele de IA cu grad ridicat de risc a unora dintre cerințele sau a tuturor cerințelor prevăzute în capitolul III secțiunea 2, ținând seama de soluțiile tehnice disponibile și de bunele practici ale sectorului care permit aplicarea unor astfel de cerințe.

- (2) Oficiul pentru IA și statele membre facilitează elaborarea de coduri de conduită privind aplicarea voluntară, inclusiv de către implementatori, a unor cerințe specifice în privința tuturor sistemelor de IA, pe baza unor obiective clare și a unor indicatori-cheie de performanță pentru a măsura îndeplinirea obiectivelor respective, inclusiv a unor elemente precum următoarele, dar fără a se limita la acestea:
- (a) elementele aplicabile prevăzute în orientările etice ale Uniunii pentru o IA de încredere;
 - (b) evaluarea și reducerea la minimum a impactului sistemelor de IA asupra durabilității mediului, inclusiv în ceea ce privește programarea eficientă din punct de vedere energetic și tehnici pentru proiectarea, antrenarea și utilizarea eficientă a IA;
 - (c) promovarea alfabetizării în domeniul IA, în special pe cea a persoanelor care se ocupă de dezvoltarea, operarea și utilizarea IA;
 - (d) facilitarea unei proiectări a sistemelor de IA care să țină seama de incluziune și diversitate, inclusiv prin crearea unor echipe de dezvoltare incluzive și diverse și promovarea participării părților interesate la acest proces;
 - (e) evaluarea și prevenirea impactului negativ al sistemelor de IA asupra persoanelor vulnerabile sau grupurilor de persoane vulnerabile, inclusiv în ceea ce privește accesibilitatea pentru persoanele cu dizabilități, precum și asupra egalității de gen.

- (3) Codurile de conduită pot fi elaborate de furnizori sau implementatori individuali de sisteme de IA sau de organizații care îi reprezintă sau de ambele, inclusiv cu implicarea oricăror părți interesate și a organizațiilor lor reprezentative, inclusiv organizațiile societății civile și mediul academic. Codurile de conduită pot acoperi unul sau mai multe sisteme de IA, ținând seama de similaritatea scopului preconizat al sistemelor relevante.
- (4) Oficiul pentru IA și statele membre țin seama de interesele și nevoile specifice ale IMM-urilor, inclusiv ale întreprinderilor nou-înființate, atunci când încurajează și facilitează elaborarea de coduri de conduită.

Articolul 96

Orientări din partea Comisiei privind punerea în aplicare a prezentului regulament

- (1) Comisia elaborează orientări privind punerea în aplicare practică a prezentului regulament, în special cu privire la:
- (a) aplicarea cerințelor și obligațiilor menționate la articolele 8-15 și la articolul 25;
 - (b) practicile interzise menționate la articolul 5;
 - (c) punerea în aplicare concretă a dispozițiilor referitoare la modificarea substanțială;
 - (d) punerea în aplicare concretă a obligațiilor de transparență prevăzute la articolul 50;

- (e) informații detaliate privind relația dintre prezentul regulament și actele legislative de armonizare ale Uniunii enumerate în anexa I, precum și alte acte legislative relevante ale Uniunii, inclusiv în ceea ce privește coerența în aplicarea acestora;
- (f) aplicarea definiției unui sistem de IA astfel cum este prevăzută la articolul 3 punctul 1.

Atunci când emite astfel de orientări, Comisia acordă o atenție deosebită nevoilor IMM-urilor, inclusiv ale întreprinderilor nou-înființate, ale autorităților publice locale și ale sectoarelor celor mai susceptibile de a fi afectate de prezentul regulament.

Orientările menționate la primul paragraf de la prezentul alineat țin seama în mod corespunzător de stadiul de avansare general recunoscut al tehnologiei în domeniul IA, precum și de standardele armonizate și specificațiile comune relevante menționate la articolele 40 și 41 sau de acele standarde armonizate sau specificații tehnice care sunt stabilite în temeiul legislației de armonizare a Uniunii.

- (2) La cererea statelor membre sau a Oficiului pentru IA ori din proprie inițiativă, Comisia actualizează orientările adoptate anterior atunci când consideră necesar.

Capitolul XI

Delegarea de competențe și procedura comitetului

Articolul 97

Exercitarea delegării

- (1) Competența de a adopta acte delegate este conferită Comisiei în condițiile prevăzute la prezentul articol.
- (2) Competența de a adopta acte delegate menționată la articolul 6 alineatele (6) și (7), la articolul 7 alineatele (1) și (3), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6), la articolul 47 alineatul (5), la articolul 51 alineatul (3), la articolul 52 alineatul (4) și la articolul 53 alineatele (5) și (6) se conferă Comisiei pe o perioadă de cinci ani de la ... [data intrării în vigoare a prezentului regulament]. Comisia elaborează un raport privind delegarea de competențe cu cel puțin nouă luni înainte de încheierea perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de timp identice, cu excepția cazului în care Parlamentul European sau Consiliul se opune prelungirii respective cu cel puțin trei luni înainte de încheierea fiecărei perioade.
- (3) Delegarea de competențe menționată la articolul 6 alineatele (6) și (7), la articolul 7 alineatele (1) și (3), la articolul 11 alineatul (3), la articolul 43 alineatele (5) și (6), la articolul 47 alineatul (5), la articolul 51 alineatul (3), la articolul 52 alineatul (4) și la articolul 53 alineatele (5) și (6) poate fi revocată oricând de Parlamentul European sau de Consiliu. O decizie de revocare pune capăt delegării de competențe specificate în decizia respectivă. Decizia produce efecte din ziua care urmează datei publicării acesteia în *Jurnalul Oficial al Uniunii Europene* sau de la o dată ulterioară menționată în decizie. Decizia nu aduce atingere actelor delegate care sunt deja în vigoare.

- (4) Înainte de adoptarea unui act delegat, Comisia consultă experții desemnați de fiecare stat membru în conformitate cu principiile prevăzute în Acordul interinstituțional din 13 aprilie 2016 privind o mai bună legiferare.
- (5) De îndată ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.
- (6) Orice act delegat adoptat în temeiul articolului 6 alineatul (6) sau (7), al articolului 7 alineatul (1) sau (3), al articolului 11 alineatul (3), al articolului 43 alineatul (5) sau (6), al articolului 47 alineatul (5), al articolului 51 alineatul (3), al articolului 52 alineatul (4) sau al articolului 53 alineatul (5) sau (6) intră în vigoare numai în cazul în care nici Parlamentul European și nici Consiliul nu au formulat obiecții în termen de trei luni de la notificarea acestuia către Parlamentul European și Consiliu sau în cazul în care, înaintea expirării termenului respectiv, Parlamentul European și Consiliul au informat Comisia că nu vor formula obiecții. Respectivul termen se prelungește cu trei luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 98

Procedura comitetului

- (1) Comisia este asistată de un comitet. Respectivul comitet reprezintă un comitet în înțelesul Regulamentului (UE) nr. 182/2011.
- (2) În cazul în care se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Capitolul XII

Sancțiuni

Articolul 99

Sancțiuni

- (1) În conformitate cu termenele și condițiile prevăzute în prezentul regulament, statele membre stabilesc normele privind sancțiunile și alte măsuri de aplicare a legii, care pot include, de asemenea, avertismente și măsuri nemonetare, aplicabile în cazul încălcării prezentului regulament de către operatori, și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare în mod corespunzător și efectiv, ținând astfel seama de orientările emise de Comisie în temeiul articolului 96. Sancțiunile prevăzute trebuie să fie efective, proporționale și cu efect de descurajare. Acestea țin seama de interesele IMM-urilor, inclusiv ale întreprinderilor nou-înființate, precum și de viabilitatea lor economică.
- (2) Statele membre îi notifică Comisiei, fără întârziere și cel târziu până la data începerii aplicării, normele privind sancțiunile și alte măsuri de aplicare a legii menționate la alineatul (1) și îi comunică acesteia fără întârziere orice modificare ulterioară a acestora.
- (3) Nerespectarea oricăreia dintre interdicțiile privind practicile în domeniul IA menționate la articolul 5 face obiectul unor amenzi administrative de până la 35 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 7 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.

- (4) Neconformitatea cu oricare dintre următoarele dispoziții referitoare la operatori sau la organisme notificate, altele decât cele prevăzute la articolul 5, face obiectul unor amenzi administrative de până la 15 000 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 3 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea:
- (a) obligațiile furnizorilor în temeiul articolului 16;
 - (b) obligațiile reprezentanților autorizați în temeiul articolului 22;
 - (c) obligațiile importatorilor în temeiul articolului 23;
 - (d) obligațiile distribuitorilor în temeiul articolului 24;
 - (e) obligațiile implementatorilor în temeiul articolului 26;
 - (f) cerințele și obligațiile organismelor notificate în temeiul articolului 31, al articolului 33 alineatele (1), (3) și (4) sau al articolului 34;
 - (g) obligațiile de transparență pentru furnizori și implementatori în temeiul articolului 50.
- (5) Furnizarea de informații incorecte, incomplete sau înșelătoare organismelor notificate sau autorităților naționale competente ca răspuns la o cerere face obiectul unor amenzi administrative de până la 7 500 000 EUR sau, în cazul în care autorul infracțiunii este o întreprindere, de până la 1 % din cifra sa de afaceri mondială totală anuală pentru exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare dintre acestea.
- (6) În cazul IMM-urilor, inclusiv al întreprinderilor nou-înființate, fiecare amendă menționată la prezentul articol nu depășește procentajele sau quantumul menționate la alineatele (3), (4) și (5), luându-se în considerare valoarea cea mai mică dintre acestea.

- (7) Atunci când se decide dacă să se impună o amendă administrativă și când se decide cu privire la cuantumul amenzii administrative în fiecare caz în parte, se iau în considerare toate circumstanțele relevante ale situației specifice și, după caz, se acordă atenție următoarelor aspecte:
- (a) natura, gravitatea și durata încălcării și a consecințelor acesteia, ținându-se seama de scopul sistemului de IA în cauză, precum și, după caz, de numărul de persoane afectate și de nivelul prejudiciilor suferite de acestea;
 - (b) dacă alte autorități de supraveghere a pieței au aplicat deja amenzi administrative aceluiși operator pentru aceeași încălcare;
 - (c) dacă alte autorități au aplicat deja amenzi administrative aceluiși operator pentru încălcări ale altor acte din dreptul Uniunii sau de drept intern, în cazul în care astfel de încălcări rezultă din aceeași activitate sau omisiune care constituie o încălcare relevantă a prezentului regulament;
 - (d) dimensiunile, cifra de afaceri anuală și cota de piață ale operatorului care a săvârșit încălcarea;
 - (e) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect ca urmare a încălcării;
 - (f) gradul de cooperare cu autoritățile naționale competente, pentru a remedia încălcarea și a atenua efectele negative posibile ale încălcării;

- (g) gradul de responsabilitate al operatorului, ținându-se seama de măsurile tehnice și organizatorice puse în aplicare de acesta;
 - (h) modul în care încălcarea a fost adusă la cunoștința autorităților naționale competente, în special dacă și, în caz afirmativ, în ce măsură operatorul a notificat încălcarea;
 - (i) dacă încălcarea a fost comisă cu intenție sau din culpă;
 - (j) orice măsură luată de operator pentru a atenua dauna suferită de persoanele afectate.
- (8) Fiecare stat membru stabilește norme cu privire la măsura în care pot fi impuse amenzi administrative autorităților și organismelor publice stabilite în statul membru respectiv.
- (9) În funcție de sistemul juridic al statelor membre, normele privind amenzile administrative pot fi aplicate astfel încât amenzile să fie impuse de instanțele naționale competente sau de alte organisme, după cum este aplicabil în statele membre respective. Aplicarea unor astfel de norme în statele membre respective are un efect echivalent.
- (10) Exercițarea competențelor în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu dreptul Uniunii și cu dreptul intern, inclusiv căi de atac judiciare eficace și dreptul la un proces echitabil.
- (11) Statele membre raportează anual Comisiei cu privire la amenzile administrative pe care le-au aplicat în cursul anului respectiv, în conformitate cu prezentul articol, precum și cu privire la orice litigii sau proceduri judiciare conexe.

Articolul 100

Amenzi administrative aplicate instituțiilor, organelor, oficiilor și agențiilor Uniunii

- (1) Autoritatea Europeană pentru Protecția Datelor poate impune amenzi administrative instituțiilor, organelor, oficiilor și agențiilor Uniunii care intră în domeniul de aplicare al prezentului regulament. Atunci când se decide dacă să se impună o amendă administrativă și când se decide cu privire la cuantumul amenzii administrative în fiecare caz în parte, se iau în considerare toate circumstanțele relevante ale situației specifice și se acordă atenția cuvenită următoarelor aspecte:
- (a) natura, gravitatea și durata încălcării și a consecințelor acesteia, ținând seama de scopul sistemului de IA în cauză, precum și, după caz, de numărul de persoane afectate și de nivelul prejudiciului suferit de acestea;
 - (b) gradul de responsabilitate al instituției, organului, oficiului sau agenției Uniunii, ținându-se seama de măsurile tehnice și organizaționale implementate de acestea;
 - (c) orice măsură luată de instituția, organul, oficiul sau agenția Uniunii pentru a atenua prejudiciul suferit de persoanele afectate;
 - (d) gradul de cooperare cu Autoritatea Europeană pentru Protecția Datelor pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării, inclusiv respectarea oricăreia dintre măsurile dispuse anterior de Autoritatea Europeană pentru Protecția Datelor împotriva instituției, organului, oficiului sau agenției Uniunii în cauză cu privire la același subiect;

- (e) eventualele încălcări anterioare similare comise de instituția, organul, oficiul sau agenția Uniunii;
 - (f) modul în care încălcarea a fost adusă la cunoștința Autorității Europene pentru Protecția Datelor, în special dacă și în ce măsură instituția, organul, oficiul sau agenția Uniunii a notificat încălcarea;
 - (g) bugetul anual al instituției, organului, oficiului sau agenției Uniunii.
- (2) Nerespectarea interdicției privind practicile în domeniul inteligenței artificiale menționate la articolul 5 face obiectul unor amenzi administrative de până la 1 500 000 EUR.
- (3) Neconformitatea sistemului de IA cu oricare dintre cerințele sau obligațiile în temeiul prezentului regulament, altele decât cele prevăzute la articolul 5, face obiectul unor amenzi administrative de până la 750 000 EUR.
- (4) Înaintea adoptării unor decizii în temeiul prezentului articol, Autoritatea Europeană pentru Protecția Datelor oferă instituției, organului, oficiului sau agenției Uniunii care face obiectul procedurilor desfășurate de Autoritatea Europeană pentru Protecția Datelor posibilitatea de a fi audiată cu privire la posibila încălcare. Autoritatea Europeană pentru Protecția Datelor își fundamentează deciziile doar pe elementele și circumstanțele asupra cărora părțile în cauză au putut formula observații. Reclamanții, dacă există, sunt implicați îndeaproape în proceduri.

- (5) Drepturile la apărare ale părților în cauză sunt pe deplin respectate în cadrul procedurilor. Părțile au drept de acces la dosarul Autorității Europene pentru Protecția Datelor, sub rezerva interesului legitim al persoanelor fizice sau al întreprinderilor în ceea ce privește protecția datelor cu caracter personal sau a secretelor comerciale ale acestora.
- (6) Fondurile colectate prin impunerea amenzilor prevăzute la prezentul articol contribuie la bugetul general al Uniunii. Amenzile nu afectează funcționarea eficace a instituției, organului, oficiului sau agenției Uniunii amendate.
- (7) Autoritatea Europeană pentru Protecția Datelor notifică anual Comisiei amenzile administrative pe care le-a impus în temeiul prezentului articol și orice litigii sau orice proceduri judiciare pe care le-a inițiat.

Articolul 101

Amenzi pentru furnizorii de modele de IA de uz general

- (1) Comisia poate impune furnizorilor de modele de IA de uz general amenzi care nu depășesc 3 % din cifra lor de afaceri mondială totală anuală pentru exercițiul financiar precedent sau 15 000 000 EUR, luându-se în considerare valoarea cea mai mare dintre acestea, atunci când Comisia constată că un furnizor, cu intenție sau din culpă:
- (a) a încălcat dispozițiile relevante din prezentul regulament;
 - (b) nu s-a conformat unei solicitări de documente sau de informații în temeiul articolului 91 sau a furnizat informații incorecte, incomplete sau înșelătoare;

- (c) nu s-a conformat unei măsuri solicitate în temeiul articolului 93;
- (d) nu a pus la dispoziția Comisiei accesul la modelul de IA de uz general sau la modelul de IA de uz general cu risc sistemic în vederea efectuării unei evaluări în temeiul articolului 92.

La stabilirea cuantumului amenzii sau al penalităților cu titlu cominatoriu, se iau în considerare natura, gravitatea și durata încălcării, ținându-se seama în mod corespunzător de principiile proporționalității și adecvării. De asemenea, Comisia ia în considerare angajamentele asumate în conformitate cu articolul 93 alineatul (3) sau în temeiul codurilor de bune practici relevante, în conformitate cu articolul 56.

- (2) Înainte de adoptarea deciziei în temeiul alineatului (1), Comisia comunică constatările sale preliminare furnizorului modelului de IA de uz general și îi oferă o posibilitate de a fi audiat.
- (3) Amenzile impuse în conformitate cu prezentul articol trebuie să fie efective, proporționale și cu efect de descurajare.
- (4) Informațiile privind amenzile impuse în temeiul prezentului articol se comunică de asemenea Consiliului IA, după caz.
- (5) Curtea de Justiție a Uniunii Europene are competența de fond de a examina deciziile Comisiei de stabilire a unei amenzi în temeiul prezentului articol. Curtea poate să anuleze, să reducă sau să majoreze amenda impusă.

- (6) Comisia adoptă acte de punere în aplicare privind modalitățile detaliate și garanțiile procedurale ale procedurilor în vederea posibilei adoptări de decizii în temeiul alineatului (1) de la prezentul articol. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 98 alineatul (2).

Capitolul XIII

Dispoziții finale

Articolul 102

Modificarea Regulamentului (CE) nr. 300/2008

La articolul 4 alineatul (3) din Regulamentul (CE) nr. 300/2008, se adaugă următorul paragraf:

„La adoptarea măsurilor detaliate referitoare la specificațiile tehnice și procedurile de aprobare și utilizare a echipamentelor de securitate în ceea ce privește sistemele de inteligență artificială în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului⁺, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 103

Modificarea Regulamentului (UE) nr. 167/2013

La articolul 17 alineatul (5) din Regulamentul (UE) nr. 167/2013, se adaugă următorul paragraf:

„La adoptarea actelor delegate în temeiul primului paragraf în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului⁺, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 104

Modificarea Regulamentului (UE) nr. 168/2013

La articolul 22 alineatul (5) din Regulamentul (UE) nr. 168/2013, se adaugă următorul paragraf:

„La adoptarea actelor delegate în temeiul primului paragraf în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului⁺, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 105
Modificarea Directivei 2014/90/UE

La articolul 8 din Directiva 2014/90/UE, se adaugă următorul alineat:

- „(5) Pentru sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului^{*,+}, atunci când își desfășoară activitățile în temeiul alineatului (1) și atunci când adoptă specificații tehnice și standarde de testare în conformitate cu alineatele (2) și (3), Comisia ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 106
Modificarea Directivei (UE) 2016/797

La articolul 5 din Directiva (UE) 2016/797, se adaugă următorul alineat:

„(12) La adoptarea actelor delegate în temeiul alineatului (1) și a actelor de punere în aplicare în temeiul alineatului (11) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului^{*,+}, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 107
Modificarea Regulamentului (UE) 2018/858

La articolul 5 din Regulamentul (UE) 2018/858, se adaugă următorul alineat:

- „(4) La adoptarea actelor delegate în temeiul alineatului (3) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului^{*,+}, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 108
Modificarea Regulamentului (UE) 2018/1139

Regulamentul (UE) 2018/1139 se modifică după cum urmează:

1. La articolul 17, se adaugă următorul alineat:

„(3) Fără a aduce atingere alineatului (2), la adoptarea actelor de punere în aplicare în temeiul alineatului (1) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului^{*,+}, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

2. La articolul 19, se adaugă următorul alineat:

„(4) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...^{++,} se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

⁺⁺ JO: a se introduce numărul prezentului regulament [2021/0106(COD)].

3. La articolul 43, se adaugă următorul alineat:

„(4) La adoptarea actelor de punere în aplicare în temeiul alineatului (1) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...⁺, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

4. La articolul 47, se adaugă următorul alineat:

„(3) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...⁺ se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

5. La articolul 57, se adaugă următorul paragraf:

„La adoptarea actelor de punere în aplicare în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...⁺ se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

6. La articolul 58, se adaugă următorul alineat:

„(3) La adoptarea actelor delegate în temeiul alineatelor (1) și (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/...⁺, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.”

⁺ JO: a se introduce numărul prezentului regulament [2021/0106(COD)].

Articolul 109
Modificarea Regulamentului (UE) 2019/2144

La articolul 11 din Regulamentul (UE) 2019/2144 se adaugă următorul alineat:

- „(3) La adoptarea actelor de punere în aplicare în temeiul alineatului (2) în ceea ce privește sistemele de inteligență artificială care sunt componente de siguranță în sensul Regulamentului (UE) 2024/... al Parlamentului European și al Consiliului⁺, se ține seama de cerințele prevăzute în capitolul III secțiunea 2 din regulamentul respectiv.

* Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ... de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L, ..., ELI: ...).”

⁺ JO: a se introduce în text numărul prezentului regulament [2021/0106(COD)] și a se completa nota de subsol corespunzătoare.

Articolul 110
Modificarea Directivei (UE) 2020/1828

În anexa I la Directiva (UE) 2020/1828 a Parlamentului European și a Consiliului⁵⁸ se adaugă următorul punct:

„(68) Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului din ...⁺ de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială) (JO L ..., ELI: ...).”

Articolul 111
Sisteme de IA deja introduse pe piață sau puse în funcțiune
și modele de IA de uz general deja introduse pe piață

(1) Fără a aduce atingere aplicării articolului 5, astfel cum se menționează la articolul 113 alineatul (3) litera (a), până la 31 decembrie 2030 se asigură conformitatea cu prezentul regulament a sistemelor de IA care sunt componente ale sistemelor informatice la scară largă instituite prin actele juridice enumerate în anexa X și care au fost introduse pe piață sau puse în funcțiune înainte de ... [36 de luni de la data intrării în vigoare a prezentului regulament].

⁵⁸ Directiva (UE) 2020/1828 a Parlamentului European și a Consiliului din 25 noiembrie 2020 privind acțiunile în reprezentare pentru protecția intereselor colective ale consumatorilor și de abrogare a Directivei 2009/22/CE (JO L 409, 4.12.2020, p. 1).

⁺ JO: a se introduce în text data și numărul prezentului regulament (2021/0106(COD)).

Cerințele prevăzute în prezentul regulament sunt luate în considerare la evaluarea fiecărui sistem informatic la scară largă instituit prin actele juridice enumerate în anexa X, care urmează să fie desfășurată astfel cum se prevede în actele juridice respective și în cazul în care actele juridice respective sunt înlocuite sau modificate.

- (2) Fără a aduce atingere aplicării articolul 5, astfel cum se menționează la articolul 113 alineatul (3) litera (a), prezentul regulament se aplică operatorilor de sisteme de IA cu grad ridicat de risc, altele decât sistemele menționate la alineatul (1) de la prezentul articol, care au fost introduse pe piață sau puse în funcțiune înainte de ... [24 de luni de la data intrării în vigoare a prezentului regulament], numai dacă, de la data respectivă, sistemele respective fac obiectul unor modificări semnificative în ceea ce privește proiectarea lor. În orice caz, furnizorii și implementatorii sistemelor de IA cu grad ridicat de risc destinate a fi utilizate de autoritățile publice iau măsurile necesare pentru a se conforma cerințelor și obligațiilor din prezentul regulament până la ... [șase ani de la data intrării în vigoare a prezentului regulament].
- (3) Furnizorii de modele de IA de uz general care au fost introduse pe piață înainte de ... [12 luni de la data intrării în vigoare a prezentului regulament] iau măsurile necesare pentru a se conforma obligațiilor prevăzute în prezentul regulament până la ... [36 de luni de la data intrării în vigoare a prezentului regulament].

Articolul 112
Evaluare și revizuire

- (1) Comisia evaluează necesitatea modificării listei din anexa III și a listei practicilor interzise în domeniul IA stabilite la articolul 5 o dată pe an după intrarea în vigoare a prezentului regulament și până la sfârșitul perioadei de delegare a competențelor stabilite la articolul 97. Comisia transmite rezultatele acestei evaluări Parlamentului European și Consiliului.
- (2) Până la ... [patru ani de la data aplicării prezentului regulament] și, ulterior, o dată la patru ani, Comisia evaluează următoarele aspecte și prezintă Parlamentului European și Consiliului un raport cu privire la acestea:
 - (a) necesitatea unor modificări de extindere a rubricilor de domeniu existente sau a adăugării unor noi rubrici de domeniu în anexa III;
 - (b) aducerea de modificări listei de sisteme de IA care necesită măsuri suplimentare de asigurare a transparenței astfel cum se menționează la articolul 50;
 - (c) aducerea de modificări care să sporească eficacitatea sistemului de supraveghere și de guvernanță.

- (3) Până la ... [cinci ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia prezintă Parlamentului European și Consiliului un raport privind evaluarea și revizuirea prezentului regulament. Raportul include o evaluare a structurii aplicării legii și a eventualei necesități ca o agenție a Uniunii să soluționeze orice deficiențe identificate. Pe baza constatărilor, raportul respectiv este însoțit, după caz, de o propunere de modificare a prezentului regulament. Rapoartele sunt făcute publice.
- (4) Rapoartele menționate la alineatul (2) acordă o atenție deosebită următoarelor aspecte:
- (a) situația resurselor financiare, tehnice și umane ale autorităților naționale competente în vederea îndeplinirii cu eficacitate a sarcinilor care le-au fost încredințate în temeiul prezentului regulament;
 - (b) situația sancțiunilor, în special a amenzilor administrative, astfel cum sunt menționate la articolul 99 alineatul (1), aplicate de statele membre în cazuri de încălcare a prezentului regulament;
 - (c) standardele armonizate adoptate și specificațiile comune elaborate pentru a sprijini prezentul regulament;
 - (d) numărul de întreprinderi care intră pe piață după începerea aplicării prezentului regulament și câte dintre acestea sunt IMM-uri.

- (5) Până la ... [patru ani de la data intrării în vigoare a prezentului regulament], Comisia evaluează funcționarea Oficiului pentru IA, dacă Oficiul pentru IA a primit suficiente atribuții și competențe pentru a-și îndeplini sarcinile și dacă ar fi relevant și necesar, pentru punerea în aplicare și respectarea în mod corespunzător a prezentului regulament, ca Oficiul pentru IA și competențele sale de executare să fie întărite și resursele sale să fie sporite. Comisia transmite un raport privind evaluarea sa Parlamentului European și Consiliului.
- (6) Până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la patru ani, Comisia prezintă Parlamentului European și Consiliului un raport privind evaluarea progreselor înregistrate în elaborarea documentelor de standardizare privind dezvoltarea eficientă din punct de vedere energetic a modelelor de IA de uz general și evaluează necesitatea unor măsuri sau acțiuni suplimentare, inclusiv a unor măsuri sau acțiuni obligatorii. Raportul se transmite Parlamentului European și Consiliului și se face public.
- (7) Până la ... [patru ani de la data intrării în vigoare a prezentului regulament] și, ulterior, o dată la trei ani, Comisia evaluează impactul și eficacitatea codurilor de conduită voluntare în ceea ce privește încurajarea aplicării cerințelor prevăzute în capitolul III secțiunea 2 pentru sistemele de IA, altele decât sistemele de IA cu grad ridicat de risc și, eventual, a altor cerințe suplimentare pentru sistemele de IA, altele decât sistemele de IA cu grad ridicat de risc, inclusiv în privința durabilității mediului.
- (8) În sensul alineatelor (1)–(7), Consiliul IA, statele membre și autoritățile naționale competente furnizează Comisiei informații la cererea acestora și fără întârzieri nejustificate.

- (9) La efectuarea evaluărilor și a revizuirilor menționate la alineatele (1)–(7), Comisia ține seama de pozițiile și constatările Consiliului IA, ale Parlamentului European, ale Consiliului, precum și ale altor organisme sau surse relevante.
- (10) Comisia transmite, dacă este necesar, propuneri corespunzătoare de modificare a prezentului regulament, în special ținând seama de evoluțiile din domeniul tehnologiei, de efectul sistemelor de IA asupra sănătății și siguranței, precum și asupra drepturilor fundamentale, și având în vedere progresele societății informaționale.
- (11) Pentru a ghida evaluările și revizuirile menționate la alineatele (1)-(7) de la prezentul articol, Oficiul pentru IA elaborează o metodologie obiectivă și participativă pentru evaluarea nivelului de risc pe baza criteriilor stabilite la articolele relevante și includerea unor sisteme noi în:
- (a) lista prevăzută în anexa III, inclusiv extinderea rubricilor de domeniu existente sau adăugarea unor noi rubrici de domeniu în anexa respectivă;
 - (b) lista de practici interzise prevăzute la articolul 5; și
 - (c) în lista de sisteme de IA care necesită măsuri suplimentare de asigurare a transparenței în temeiul articolului 50.
- (12) Orice modificare a prezentului regulament în temeiul alineatului (10) sau orice act delegat ori de punere în aplicare relevant, care vizează actele legislative sectoriale de armonizare ale Uniunii enumerate în secțiunea B din anexa I, ia în considerare particularitățile de reglementare ale fiecărui sector și mecanismele și autoritățile existente de guvernanță, de evaluare a conformității și de aplicare a legii instituite în actele respective.

- (13) Până la ... [șapte ani de la data intrării în vigoare a prezentului regulament], Comisia efectuează o evaluare aplicării prezentului regulament și prezintă un raport referitor la aceasta Parlamentului European, Consiliului și Comitetului Economic și Social European, vizând primii ani de aplicare a prezentului regulament. Pe baza constatărilor, raportul este însoțit, după caz, de o propunere de modificare a prezentului regulament cu privire la structura aplicării legii și la necesitatea ca o agenție a Uniunii să soluționeze deficiențele identificate.

Articolul 113

Intrare în vigoare și aplicare

Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Acesta se aplică de la ... [24 de luni de la data intrării în vigoare a prezentului regulament].

Cu toate acestea:

- (a) capitolele I și II se aplică de la ... [șase luni de la data intrării în vigoare a prezentului regulament];
- (b) Capitolul III secțiunea 4, capitolul V, capitolul VII, capitolul XII și articolul 78 se aplică de la ... [12 luni de la data intrării în vigoare a prezentului regulament], cu excepția articolului 101;

- (c) Articolul 6 alineatul (1) și obligațiile corespunzătoare din prezentul regulament se aplică de la ... [36 de luni de la data intrării în vigoare a prezentului regulament].

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles,

Pentru Parlamentul European
Președinta

Pentru Consiliu
Președintele

ANEXA I

Lista legislației de armonizare a Uniunii

Secțiunea A – Lista actelor legislative de armonizare ale Uniunii pe baza noului cadru legislativ

1. Directiva 2006/42/CE a Parlamentului European și a Consiliului din 17 mai 2006 privind echipamentele tehnice și de modificare a Directivei 95/16/CE (JO L 157, 9.6.2006, p. 24);
2. Directiva 2009/48/CE a Parlamentului European și a Consiliului din 18 iunie 2009 privind siguranța jucăriilor (JO L 170, 30.6.2009, p. 1);
3. Directiva 2013/53/UE a Parlamentului European și a Consiliului din 20 noiembrie 2013 privind ambarcațiunile de agrement și motovehiculele nautice și de abrogare a Directivei 94/25/CE (JO L 354, 28.12.2013, p. 90);
4. Directiva 2014/33/UE a Parlamentului European și a Consiliului din 26 februarie 2014 de armonizare a legislațiilor statelor membre referitoare la ascensoare și la componentele de siguranță pentru ascensoare (JO L 96, 29.3.2014, p. 251);
5. Directiva 2014/34/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind armonizarea legislațiilor statelor membre referitoare la echipamentele și sistemele de protecție destinate utilizării în atmosfere potențial explozive (JO L 96, 29.3.2014, p. 309);

6. Directiva 2014/53/UE a Parlamentului European și a Consiliului din 16 aprilie 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor radio și de abrogare a Directivei 1999/5/CE (JO L 153, 22.5.2014, p. 62);
7. Directiva 2014/68/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind armonizarea legislației statelor membre referitoare la punerea la dispoziție pe piață a echipamentelor sub presiune (JO L 189, 27.6.2014, p. 164);
8. Regulamentul (UE) 2016/424 al Parlamentului European și al Consiliului din 9 martie 2016 privind instalațiile pe cablu și de abrogare a Directivei 2000/9/CE (JO L 81, 31.3.2016, p. 1);
9. Regulamentul (UE) 2016/425 al Parlamentului European și al Consiliului din 9 martie 2016 privind echipamentele individuale de protecție și de abrogare a Directivei 89/686/CEE a Consiliului (JO L 81, 31.3.2016, p. 51);
10. Regulamentul (UE) 2016/426 al Parlamentului European și al Consiliului din 9 martie 2016 privind aparatele consumatoare de combustibili gazoși și de abrogare a Directivei 2009/142/CE (JO L 81, 31.3.2016, p. 99);
11. Regulamentul (UE) 2017/745 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale, de modificare a Directivei 2001/83/CE, a Regulamentului (CE) nr. 178/2002 și a Regulamentului (CE) nr. 1223/2009 și de abrogare a Directivelor 90/385/CEE și 93/42/CEE ale Consiliului (JO L 117, 5.5.2017, p. 1);

12. Regulamentul (UE) 2017/746 al Parlamentului European și al Consiliului din 5 aprilie 2017 privind dispozitivele medicale pentru diagnostic *in vitro* și de abrogare a Directivei 98/79/CE și a Deciziei 2010/227/UE a Comisiei (JO L 117, 5.5.2017, p. 176).

Secțiunea B. Lista altor acte legislative de armonizare ale Uniunii

13. Regulamentul (CE) nr. 300/2008 al Parlamentului European și al Consiliului din 11 martie 2008 privind norme comune în domeniul securității aviației civile și de abrogare a Regulamentului (CE) nr. 2320/2002 (JO L 97, 9.4.2008, p. 72);
14. Regulamentul (UE) nr. 168/2013 al Parlamentului European și al Consiliului din 15 ianuarie 2013 privind omologarea și supravegherea pieței pentru vehiculele cu două sau trei roți și pentru cvadricicluri (JO L 60, 2.3.2013, p. 52);
15. Regulamentul (UE) nr. 167/2013 al Parlamentului European și al Consiliului din 5 februarie 2013 privind omologarea și supravegherea pieței pentru vehiculele agricole și forestiere (JO L 60, 2.3.2013, p. 1);
16. Directiva 2014/90/UE a Parlamentului European și a Consiliului din 23 iulie 2014 privind echipamentele maritime și de abrogare a Directivei 96/98/CE a Consiliului (JO L 257, 28.8.2014, p. 146);
17. Directiva (UE) 2016/797 a Parlamentului European și a Consiliului din 11 mai 2016 privind interoperabilitatea sistemului feroviar în Uniunea Europeană (JO L 138, 26.5.2016, p. 44);

18. Regulamentul (UE) 2018/858 al Parlamentului European și al Consiliului din 30 mai 2018 privind omologarea și supravegherea pieței autovehiculelor și remorcilor acestora, precum și ale sistemelor, componentelor și unităților tehnice separate destinate vehiculelor respective, de modificare a Regulamentelor (CE) nr. 715/2007 și (CE) nr. 595/2009 și de abrogare a Directivei 2007/46/CE (JO L 151, 14.6.2018, p. 1);
19. Regulamentul (UE) 2019/2144 al Parlamentului European și al Consiliului din 27 noiembrie 2019 privind cerințele pentru omologarea de tip a autovehiculelor și remorcilor acestora, precum și a sistemelor, componentelor și unităților tehnice separate destinate unor astfel de vehicule, în ceea ce privește siguranța generală a acestora și protecția ocupanților vehiculului și a utilizatorilor vulnerabili ai drumurilor, de modificare a Regulamentului (UE) 2018/858 al Parlamentului European și al Consiliului și de abrogare a Regulamentelor (CE) nr. 78/2009, (CE) nr. 79/2009 și (CE) nr. 661/2009 ale Parlamentului European și ale Consiliului și a Regulamentelor (CE) nr. 631/2009, (UE) nr. 406/2010, (UE) nr. 672/2010, (UE) nr. 1003/2010, (UE) nr. 1005/2010, (UE) nr. 1008/2010, (UE) nr. 1009/2010, (UE) nr. 19/2011, (UE) nr. 109/2011, (UE) nr. 458/2011, (UE) nr. 65/2012, (UE) nr. 130/2012, (UE) nr. 347/2012, (UE) nr. 351/2012, (UE) nr. 1230/2012 și (UE) 2015/166 ale Comisiei (JO L 325, 16.12.2019, p. 1);

20. Regulamentul (UE) 2018/1139 al Parlamentului European și al Consiliului din 4 iulie 2018 privind normele comune în domeniul aviației civile și de înființare a Agenției Uniunii Europene pentru Siguranța Aviației, de modificare a Regulamentelor (CE) nr. 2111/2005, (CE) nr. 1008/2008, (UE) nr. 996/2010, (UE) nr. 376/2014 și a Directivelor 2014/30/UE și 2014/53/UE ale Parlamentului European și ale Consiliului, precum și de abrogare a Regulamentelor (CE) nr. 552/2004 și (CE) nr. 216/2008 ale Parlamentului European și ale Consiliului și a Regulamentului (CEE) nr. 3922/91 al Consiliului (JO L 212, 22.8.2018, p. 1), în ceea ce privește proiectarea, producerea și introducerea pe piață a aeronavelor menționate la articolul 2 alineatul (1) literele (a) și (b), în cazul aeronavelor fără pilot la bord și al motoarelor, elicelor, pieselor și echipamentelor acestora de control de la distanță.
-

ANEXA II

Lista infracțiunilor menționate la articolul 5 alineatul (1) primul paragraf litera (h) punctul (iii)

Infracțiunile menționate la articolul 5 alineatul (1) primul paragraf litera (h) punctul (iii):

- terorism,
- trafic de ființe umane,
- exploatare sexuală a copiilor și pornografie infantilă,
- trafic ilicit de stupeficante sau de substanțe psihotrope,
- trafic ilicit de arme, muniții sau substanțe explozive,
- omor, vătămare corporală gravă,
- trafic ilicit de organe sau țesuturi umane,
- trafic ilicit de materiale nucleare sau radioactive,
- răpire, lipsire de libertate în mod ilegal sau luare de ostatici,
- infracțiuni de competența Curții Penale Internaționale,
- sechestrare ilicită de aeronave sau de nave,

- viol,
 - infracțiuni împotriva mediului,
 - jaf organizat sau armat,
 - sabotaj,
 - participare la o organizație criminală implicată în una sau mai multe dintre infracțiunile enumerate mai sus.
-

ANEXA III

Sisteme de IA cu grad ridicat de risc menționate la articolul 6 alineatul (2)

Sistemele de IA cu grad ridicat de risc conform articolului 6 alineatul (2) sunt sistemele de IA aparținând oricăruia dintre următoarele domenii:

1. Biometrie, în măsura în care utilizarea acesteia este permisă în temeiul dreptului Uniunii sau intern relevant:

- (a) sisteme de identificare biometrică la distanță.

Acestea nu includ sistemele de IA destinate a fi utilizate pentru verificarea biometrică al cărei unic scop este de a confirma că o anumită persoană fizică este persoana care susține că este;

- (b) sisteme de IA destinate a fi utilizate pentru clasificarea biometrică, în funcție de atribute sau caracteristici sensibile ori protejate, pe baza deducerii acestor atribute sau caracteristici;

- (c) sisteme de IA destinate a fi utilizate pentru recunoașterea emoțiilor.

2. Infrastructură critică: sisteme de IA destinate a fi utilizate drept componente de siguranță în gestionarea și exploatarea infrastructurii digitale critice, a traficului rutier sau a aprovizionării cu apă, gaz, încălzire ori energie electrică.

3. Educație și formare profesională:

- (a) sisteme de IA destinate a fi utilizate pentru a stabili accesul ori admisia sau pentru a repartiza persoane fizice la instituțiile de învățământ și formare profesională la toate nivelurile;
- (b) sisteme de IA destinate a fi utilizate pentru a evalua rezultatele învățării, inclusiv atunci când acestea sunt utilizate pentru a orienta procesul de învățare al persoanelor fizice în instituțiile de învățământ și formare profesională la toate nivelurile;
- (c) sisteme de IA destinate a fi utilizate în scopul evaluării nivelului adecvat de educație pe care o persoană îl va primi sau îl va putea accesa, în contextul sau în cadrul instituțiilor de învățământ și formare profesională la toate nivelurile;
- (d) sisteme de IA destinate a fi utilizate pentru monitorizarea și detectarea comportamentului interzis al elevilor și studenților în timpul testelor, în contextul sau în cadrul instituțiilor de educație și formare profesională la toate nivelurile.

4. Ocuparea forței de muncă, gestionarea lucrătorilor și accesul la activități independente:

- (a) sisteme de IA destinate a fi utilizate pentru recrutarea sau selectarea persoanelor fizice, în special pentru a plasa anunțuri de angajare direcționate în mod specific, pentru a analiza și a filtra candidaturile pentru locuri de muncă și pentru a evalua candidații;

- (b) sisteme de IA destinate a fi utilizate pentru a lua decizii care afectează termenii relațiilor legate de muncă, promovarea și încetarea relațiilor contractuale legate de muncă, pentru a aloca sarcini pe baza comportamentului individual sau a trăsăturilor ori caracteristicilor personale sau pentru a monitoriza și evalua performanța și comportamentul persoanelor aflate în astfel de relații.

5. Accesul la servicii private esențiale și la servicii și beneficii publice esențiale, precum și posibilitatea de a beneficia de acestea:

- (a) sisteme de IA destinate a fi utilizate de autoritățile publice sau în numele autorităților publice pentru a evalua eligibilitatea persoanelor fizice pentru prestații și servicii de asistență publică esențiale, inclusiv servicii de îngrijiri de sănătate, precum și pentru a acorda, a reduce, a revoca sau a recupera astfel de prestații și servicii;
- (b) sisteme de IA destinate a fi utilizate pentru a evalua bonitatea persoanelor fizice sau pentru a stabili punctajul lor de credit, cu excepția sistemelor de IA utilizate în scopul detectării fraudelor financiare;
- (c) sisteme de IA destinate a fi utilizate pentru evaluarea riscurilor și stabilirea prețurilor în ceea ce privește persoanele fizice în cazul asigurărilor de viață și de sănătate;
- (d) sisteme de IA destinate pentru a evalua și a clasifica apelurile de urgență efectuate de persoane fizice sau pentru a distribui ori pentru a stabili prioritatea în distribuirea serviciilor de primă intervenție de urgență, inclusiv de către poliție, pompieri și asistența medicală, precum și în cadrul sistemelor de triaj de urgență pentru pacienți.

6. Aplicarea legii, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii sau intern relevant:
- (a) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii sau în numele acestora pentru a evalua riscul ca o persoană fizică să devină victima unor infracțiuni;
 - (b) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii ca poligrafe sau instrumente similare sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii;
 - (c) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru a evalua fiabilitatea probelor în cursul investigării sau al urmăririi penale a infracțiunilor;
 - (d) sisteme de IA destinate a fi utilizate de către autoritățile de aplicare a legii sau în numele acestora de către instituțiile, organele, oficiile sau agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru evaluarea riscului ca o persoană fizică să comită infracțiuni sau să recidiveze, nu doar pe baza creării de profiluri ale persoanelor fizice, astfel cum se menționează la articolul 3 alineatul (4) din Directiva (UE) 2016/680, sau pentru a evalua trăsături și caracteristici de personalitate ori comportamentul infracțional anterior al unor persoane fizice sau grupuri;

- (e) sisteme de IA destinate a fi utilizate de către sau în numele autorităților de aplicare a legii sau de către instituțiile, organele, oficiile ori agențiile Uniunii în sprijinul autorităților de aplicare a legii pentru crearea de profiluri ale persoanelor fizice, astfel cum se menționează la articolul 3 alineatul (4) din Directiva (UE) 2016/680, în cursul depistării, investigării sau urmăririi penale a infracțiunilor.

7. Migrație, azil și gestionare a controlului la frontiere, în măsura în care utilizarea lor este permisă în temeiul dreptului Uniunii sau intern relevant:

- (a) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii drept poligrafe sau instrumente similare;
- (b) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii pentru evaluarea unui risc, inclusiv a unui risc de securitate, a unui risc de migrație ilegală sau a unui risc pentru sănătate din partea unei persoane fizice care intenționează să intre sau care a intrat pe teritoriul unui stat membru;
- (c) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile ori agențiile Uniunii pentru a asista autoritățile publice competente în examinarea cererilor de azil, de viză sau de permise de ședere și a plângerilor aferente în ceea ce privește eligibilitatea persoanelor fizice care solicită un statut, inclusiv în evaluările conexe ale fiabilității probelor;

- (d) sisteme de IA destinate a fi utilizate de către sau în numele autorităților publice competente sau de către instituțiile, organele, oficiile sau agențiile Uniunii, în contextul migrației, azilului sau gestionării controlului la frontiere, în scopul detectării, recunoașterii sau identificării persoanelor fizice, cu excepția verificării documentelor de călătorie.

8. Administrarea justiției și procesele democratice:

- (a) sisteme de IA destinate a fi utilizate de către sau în numele unei autorități judiciare pentru a asista o autoritate judiciară în cercetarea și interpretarea faptelor sau a legii, precum și în aplicarea legii la un set concret de fapte sau destinate a fi utilizate în mod similar în soluționarea alternativă a litigiilor;
- (b) sisteme de IA destinate a fi utilizate pentru a influența rezultatul unei alegeri sau al unui referendum ori comportamentul de vot al persoanelor fizice în exercitarea votului lor la alegeri sau referendumuri. Acestea nu includ sistemele de IA la ale căror rezultate nu sunt expuse direct persoane fizice, cum ar fi instrumentele utilizate pentru organizarea, optimizarea sau structurarea campaniilor politice din punct de vedere administrativ sau logistic.

ANEXA IV

Documentația tehnică menționată la articolul 11 alineatul (1)

Documentația tehnică menționată la articolul 11 alineatul (1) conține cel puțin următoarele informații, aplicabile sistemului de IA relevant:

1. O descriere generală a sistemului de IA, incluzând:
 - (a) scopul său preconizat, numele/denumirea furnizorului și versiunea sistemului, care reflectă relația sa cu versiunile anterioare;
 - (b) modul în care sistemul de IA interacționează sau poate fi utilizat pentru a interacționa cu hardware-ul sau cu software-ul, inclusiv cu alte sisteme de IA care nu fac parte din sistemul de IA în sine, după caz;
 - (c) versiunile software-ului sau ale firmware-ului relevant și orice cerințe legate de actualizările versiunilor;
 - (d) descrierea tuturor formelor sub care sistemul de IA este introdus pe piață sau este pus în funcțiune, cum ar fi pachete software integrate în hardware, sisteme care pot fi descărcate sau IPA;
 - (e) descrierea hardware-ului pe care urmează să funcționeze sistemul de IA;
 - (f) în cazul în care sistemul de IA este o componentă a unor produse, fotografii sau ilustrații care prezintă caracteristici externe, marcajele și dispunerea internă a produselor respective;

- (g) o descriere de bază a interfeței cu utilizatorul furnizate implementatorului;
 - (h) instrucțiuni de utilizare pentru implementator și o descriere de bază a interfeței cu utilizatorul furnizate implementatorului, după caz;
2. O descriere detaliată a elementelor sistemului de IA și a procesului de dezvoltare a acestuia, incluzând:
- (a) metodele și etapele parcurse pentru dezvoltarea sistemului de IA, inclusiv, dacă este cazul, recurgerea la sisteme sau instrumente preantrenate furnizate de terți și modul în care acestea au fost utilizate, integrate sau modificate de către furnizor;
 - (b) specificațiile de proiectare ale sistemului, și anume logica generală a sistemului de IA și a algoritmilor; principalele opțiuni de proiectare, incluzând justificarea și ipotezele asumate, inclusiv în ceea ce privește persoanele sau grupurile de persoane în legătură cu care se intenționează să fie utilizat sistemul; principalele opțiuni de clasificare; ce anume este proiectat să optimizeze sistemul și relevanța diverșilor parametri; descrierea rezultatelor preconizate ale sistemului și a calității preconizate a acestora; deciziile cu privire la orice posibil compromis făcut în ceea ce privește soluțiile tehnice adoptate în vederea respectării cerințelor prevăzute în capitolul III secțiunea 2;
 - (c) descrierea arhitecturii sistemului, care explică modul în care componentele de software se bazează una pe alta sau se susțin reciproc și se integrează în prelucrarea generală; resursele de calcul utilizate pentru dezvoltarea, antrenarea, testarea și validarea sistemului de IA;

- (d) după caz, cerințele în materie de date în ceea ce privește fișele tehnice care descriu metodologiile și tehnicile de antrenare și seturile de date de antrenament utilizate, inclusiv o descriere generală a acestor seturi de date, informații privind proveniența, domeniul de aplicare și principalele caracteristici ale acestora; modul în care au fost obținute și selectate datele; proceduri de etichetare (de exemplu, pentru învățarea supervizată), metodologii de curățare a datelor (de exemplu, detectarea valorilor aberante);
- (e) evaluarea măsurilor de supraveghere umană necesare în conformitate cu articolul 14, inclusiv o evaluare a măsurilor tehnice necesare pentru a facilita interpretarea rezultatelor sistemelor de IA de către implementatori, în conformitate cu articolul 13 alineatul (3) litera (d);
- (f) după caz, o descriere detaliată a modificărilor prestabilite ale sistemului de IA și ale performanței acestuia, împreună cu toate informațiile relevante referitoare la soluțiile tehnice adoptate pentru a asigura conformitatea continuă a sistemului de IA cu cerințele relevante prevăzute în capitolul III secțiunea 2;
- (g) procedurile de validare și testare utilizate, inclusiv informații cu privire la datele de validare și testare utilizate și la principalele caracteristici ale acestora; indicatorii utilizați pentru a măsura acuratețea, robustețea și conformitatea cu alte cerințe relevante prevăzute în capitolul III secțiunea 2, precum și impactul potențial discriminatoriu; jurnalele de testare și toate rapoartele de testare datate și semnate de persoanele responsabile, inclusiv în ceea ce privește modificările prestabilite menționate la litera (f);
- (h) măsurile de securitate cibernetică instituite;

3. Informații detaliate privind monitorizarea, funcționarea și controlul sistemului de IA, în special în ceea ce privește: capacitățile și limitările sale legate de performanță, inclusiv gradele de acuratețe pentru anumite persoane sau grupuri de persoane pentru care se intenționează să se utilizeze sistemul respectiv, precum și nivelul general preconizat de acuratețe în raport cu scopul preconizat; rezultatele neintenționate previzibile și sursele de riscuri pentru sănătate, siguranță, drepturile fundamentale și în materie de discriminare, având în vedere scopul preconizat al sistemului de IA; măsurile de supraveghere umană necesare în conformitate cu articolul 14, inclusiv măsurile tehnice instituite pentru a facilita interpretarea rezultatelor sistemelor de IA de către implementatori; specificații privind datele de intrare, după caz;
4. O descriere a gradului de adecvare a indicatorilor de performanță pentru sistemul de IA specific;
5. O descriere detaliată a sistemului de gestionare a riscurilor în conformitate cu articolul 9;
6. O descriere a modificărilor relevante aduse de furnizor sistemului de-a lungul ciclului său de viață;
7. O listă a standardelor armonizate aplicate integral sau parțial, ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*, iar în cazul în care nu au fost aplicate astfel de standarde armonizate, o descriere detaliată a soluțiilor adoptate pentru a se îndeplini cerințele prevăzute în capitolul III secțiunea 2, inclusiv o listă a altor standarde și specificații tehnice relevante aplicate;
8. O copie a declarației de conformitate UE menționată la articolul 47;
9. O descriere detaliată a sistemului instituit pentru evaluarea performanței sistemului de IA în etapa ulterioară introducerii pe piață în conformitate cu articolul 72, inclusiv planul de monitorizare ulterioară introducerii pe piață menționat la articolul 72 alineatul (3).

ANEXA V

Declarația de conformitate UE

Declarația de conformitate UE menționată la articolul 47 conține toate informațiile următoare:

1. Denumirea și tipul sistemului de IA și orice referință suplimentară lipsită de ambiguitate care permite identificarea și trasabilitatea sistemului de IA;
2. Numele/denumirea și adresa furnizorului sau, după caz, ale reprezentantului autorizat al acestuia;
3. O declarație potrivit căreia declarația de conformitate UE menționată la articolul 47 este emisă pe răspunderea exclusivă a furnizorului;
4. O declarație potrivit căreia sistemul de IA este conform cu prezentul regulament și, după caz, cu orice alt act legislativ relevant al Uniunii care prevede emiterea declarației de conformitate UE menționată la articolul 47;
5. Dacă un sistem de IA implică prelucrarea de date cu caracter personal, o declarație că sistemul de IA respectiv este conform cu Regulamentele (UE) 2016/679 și (UE) 2018/1725 și Directiva (UE) 2016/680;
6. Trimiteri la toate standardele armonizate relevante utilizate sau la orice altă specificație comună în legătură cu care se declară conformitatea;

7. După caz, denumirea și numărul de identificare ale organismului notificat, o descriere a procedurii de evaluare a conformității efectuate și identificarea certificatului eliberat;
 8. Locul și data emiterii declarației, numele și funcția persoanei care a semnat-o, precum și o indicație pentru cine sau în numele cui a semnat, semnătura.
-

ANEXA VI

Procedura de evaluare a conformității bazată pe control intern

1. Procedura de evaluare a conformității bazată pe control intern este procedura de evaluare a conformității realizată pe baza punctelor 2, 3 și 4.
 2. Furnizorul verifică dacă sistemul de management al calității instituit respectă cerințele de la articolul 17.
 3. Furnizorul examinează informațiile conținute în documentația tehnică pentru a evalua conformitatea sistemului de IA cu cerințele esențiale relevante prevăzute în capitolul III secțiunea 2.
 4. Furnizorul verifică, de asemenea, dacă procesul de proiectare și dezvoltare a sistemului de IA și monitorizarea ulterioară introducerii pe piață a acestuia, astfel cum se menționează la articolul 72, sunt în concordanță cu documentația tehnică.
-

ANEXA VII

Evaluarea conformității pe baza unui sistem de management al calității și a examinării documentației tehnice

1. Introducere

Evaluarea conformității pe baza unui sistem de management al calității și a examinării documentației tehnice este procedura de evaluare a conformității realizată pe baza punctelor 2-5.

2. Prezentare generală

Sistemul de management al calității aprobat pentru proiectarea, dezvoltarea și testarea sistemelor de IA în temeiul articolului 17 este examinat în conformitate cu punctul 3 și face obiectul supravegherii menționate la punctul 5. Documentația tehnică a sistemului de IA se examinează în conformitate cu punctul 4.

3. Sistemul de management al calității

3.1. Cererea furnizorului include:

- (a) numele/denumirea și adresa furnizorului, iar, dacă cererea este depusă de către un reprezentant autorizat, și numele și adresa acestuia;
- (b) lista sistemelor de IA care fac obiectul aceluiași sistem de management al calității;
- (c) documentația tehnică a fiecărui sistem de IA pentru care se aplică același sistem de management al calității;

- (d) documentația privind sistemul de management al calității, care acoperă toate aspectele enumerate la articolul 17;
- (e) o descriere a procedurilor instituite pentru a se asigura că sistemul de management al calității continuă să fie adecvat și eficace;
- (f) o declarație scrisă care să specifice că nu a fost depusă o cerere identică la un alt organism notificat.

3.2. Sistemul de management al calității este evaluat de organismul notificat, care stabilește dacă acesta satisface cerințele menționate la articolul 17.

Decizia se notifică furnizorului sau reprezentantului autorizat al acestuia.

Notificarea respectivă trebuie să cuprindă concluziile evaluării sistemului de management al calității și decizia de evaluare motivată.

3.3. Sistemul de management al calității, astfel cum a fost aprobat, continuă să fie pus în aplicare și menținut de către furnizor astfel încât să rămână adecvat și eficient.

3.4. Orice modificare preconizată a sistemului aprobat de management al calității sau a listei sistemelor de IA cărora li se aplică acesta este adusă la cunoștința organismului notificat, de către furnizor.

Modificările propuse sunt examinate de organismul notificat, care decide dacă sistemul de management al calității modificat îndeplinește în continuare cerințele menționate la punctul 3.2 sau dacă este necesară o reevaluare.

Organismul notificat înștiințează furnizorul cu privire la decizia pe care a luat-o.

Notificarea respectivă trebuie să cuprindă concluziile examinării modificărilor și decizia de evaluare motivată.

4. Controlul documentației tehnice

4.1. În plus față de cererea menționată la punctul 3, furnizorul depune o cerere la un organism notificat ales de acesta pentru evaluarea documentației tehnice referitoare la sistemul de IA pe care furnizorul intenționează să îl introducă pe piață sau să îl pună în funcțiune și căruia i se aplică sistemul de management al calității menționat la punctul 3.

4.2. Cererea include:

- (a) numele/denumirea și adresa furnizorului;
- (b) o declarație scrisă care să precizeze că nu a fost depusă o cerere identică la un alt organism notificat;
- (c) documentația tehnică menționată în anexa IV.

4.3. Documentația tehnică este examinată de organismul notificat. Atunci când acest lucru este relevant, și limitându-se la ceea ce este necesar pentru a-și îndeplini sarcinile, organismului notificat i se acordă acces deplin la seturile de date de antrenament, de validare și de testare utilizate, inclusiv, după caz și sub rezerva unor garanții de securitate, prin IPA sau prin alte mijloace și instrumente tehnice relevante care permit accesul de la distanță.

- 4.4. La examinarea documentației tehnice, organismul notificat poate solicita furnizorului să prezinte dovezi suplimentare sau să efectueze teste suplimentare pentru a permite o evaluare adecvată a conformității sistemului de IA cu cerințele prevăzute în capitolul III secțiunea 2. Ori de câte ori organismul notificat nu este satisfăcut de testele efectuate de furnizor, organismul notificat efectuează el însuși direct teste adecvate, după caz.
- 4.5. În cazul în care este necesar pentru a evalua conformitatea sistemului de IA cu grad ridicat de risc cu cerințele prevăzute în capitolul III secțiunea 2, după ce toate celelalte modalități rezonabile de verificare a conformității au fost epuizate ori s-au dovedit a fi insuficiente și în urma unei cereri motivate, organismului notificat i se acordă, de asemenea, acces la modelele de antrenament sau modelele antrenate ale sistemului de IA, inclusiv la parametrii săi relevanți. Acest acces face obiectul dreptului existent al Uniunii privind protecția proprietății intelectuale și al secretelor comerciale.
- 4.6. Decizia organismului notificat se notifică furnizorului sau reprezentantului autorizat al acestuia. Notificarea respectivă trebuie să cuprindă concluziile examinării documentației tehnice și decizia de evaluare motivată.

În cazul în care sistemul de IA este în conformitate cu cerințele prevăzute în capitolul III secțiunea 2, organismul notificat eliberează un certificat de evaluare a documentației tehnice al Uniunii. Certificatul indică numele/denumirea și adresa furnizorului, concluziile examinării, condițiile (dacă există) de valabilitate și datele necesare de identificare a sistemului de IA.

Certificatul și anexele sale conțin toate informațiile relevante care să permită evaluarea conformității sistemului de IA și controlul sistemului de IA în timpul utilizării acestuia, după caz.

În cazul în care sistemul de IA nu este conform cu cerințele prevăzute în capitolul III secțiunea 2, organismul notificat refuză eliberarea unui certificat de evaluare a documentației tehnice al Uniunii și informează solicitantul în consecință, indicând motivele detaliate ale refuzului său.

În cazul în care sistemul de IA nu îndeplinește cerința referitoare la datele utilizate pentru antrenarea sa, va fi necesară reantrenarea sistemului de IA înaintea depunerii cererii pentru o nouă evaluare a conformității. În acest caz, decizia de evaluare motivată a organismului notificat prin care se refuză eliberarea certificatului de evaluare a documentației tehnice al Uniunii conține considerații specifice privind calitatea datelor utilizate pentru antrenarea sistemului de IA, în special cu privire la motivele neconformității.

- 4.7. Orice modificare a sistemului de IA care ar putea afecta conformitatea sistemului de IA cu cerințele sau cu scopul preconizat al acestuia este evaluată de organismul notificat care a eliberat certificatul de evaluare a documentației tehnice al Uniunii. Furnizorul informează organismul notificat în cauză cu privire la intenția sa de a introduce oricare dintre modificările menționate anterior sau în cazul în care ia cunoștință în alt mod de apariția unor astfel de modificări. Organismul notificat evaluează modificările planificate și decide pentru care din acestea este necesară o nouă evaluare a conformității în concordanță cu articolul 43 alineatul (4) sau dacă acestea ar putea fi abordate prin intermediul unui supliment la certificatul de evaluare a documentației tehnice al Uniunii. În acest din urmă caz, organismul notificat evaluează modificările, îi notifică furnizorului decizia sa și, în cazul în care modificările sunt aprobate, îi eliberează un supliment la certificatul de evaluare a documentației tehnice al Uniunii.

5. Supravegherea sistemului de management al calității aprobat.
- 5.1. Scopul supravegherii efectuate de organismul notificat menționat la punctul 3 este de a asigura faptul că furnizorul respectă în mod corespunzător termenele și condițiile sistemului de management al calității aprobat.
- 5.2. În scopul evaluării, furnizorul permite organismului notificat să aibă acces la sediul în care are loc proiectarea, dezvoltarea sau testarea sistemelor de IA. În plus, furnizorul comunică organismului notificat toate informațiile necesare.
- 5.3. Organismul notificat efectuează misiuni de audit periodice, pentru a se asigura că furnizorul menține și aplică sistemul de management al calității, și prezintă furnizorului un raport de audit. În contextul acestor audituri, organismul notificat poate efectua teste suplimentare ale sistemelor de IA pentru care a fost emis un certificat de evaluare a documentației tehnice al Uniunii.
-

ANEXA VIII

Informațiile care trebuie să fie prezentate la înregistrarea sistemelor de IA cu grad ridicat de risc în conformitate cu articolul 49

Secțiunea A – Informațiile care trebuie să fie prezentate de furnizorii de sisteme de IA cu grad ridicat de risc în conformitate cu articolul 49 alineatul (1)

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la sistemele de IA cu grad ridicat de risc care se înregistrează în conformitate cu articolul 49 alineatul (1):

1. Numele/denumirea, adresa și datele de contact ale furnizorului;
2. În cazul în care transmiterea informațiilor este efectuată de o altă persoană în numele furnizorului, numele, adresa și datele de contact ale persoanei respective;
3. Numele, adresa și datele de contact ale reprezentantului autorizat, după caz;
4. Denumirea comercială a sistemului de IA și orice referință suplimentară lipsită de ambiguitate care permite identificarea și trasabilitatea sistemului de IA;
5. O descriere a scopului preconizat al sistemului de IA și a componentelor și funcțiilor sprijinite prin acest sistem de IA;
6. O descriere de bază și concisă a informațiilor utilizate de sistem (date, date de intrare) și a logicii sale de funcționare;

7. Statutul sistemului de IA (pe piață sau în funcțiune; nu mai este pe piață/în funcțiune, rechemat);
8. Tipul, numărul și data expirării certificatului eliberat de organismul notificat și denumirea sau numărul de identificare al organismului notificat respectiv, după caz;
9. O copie scanată a certificatului menționat la punctul 8, după caz;
10. Orice stat membru în care sistemul de IA a fost introdus pe piață, pus în funcțiune sau pus la dispoziție în Uniune;
11. O copie a declarației de conformitate UE prevăzută la articolul 47;
12. Instrucțiuni de utilizare electronice; aceste informații nu se furnizează pentru sistemele de IA cu grad ridicat de risc în domeniul aplicării legii și al migrației, al azilului și al gestionării controlului la frontiere menționate în anexa III punctele 1, 6 și 7;
13. Un URL pentru informații suplimentare (opțional).

Secțiunea B – Informațiile care trebuie să fie prezentate de furnizorii de sisteme de IA
cu grad ridicat de risc în conformitate cu articolul 49 alineatul (2)

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la sistemele de IA care se înregistrează în conformitate cu articolul 49 alineatul (2):

1. Numele/denumirea, adresa și datele de contact ale furnizorului;
2. În cazul în care transmiterea informațiilor este efectuată de o altă persoană în numele furnizorului, numele, adresa și datele de contact ale persoanei respective;
3. Numele, adresa și datele de contact ale reprezentantului autorizat, după caz;
4. Denumirea comercială a sistemului de IA și orice referință suplimentară lipsită de ambiguitate care permite identificarea și trasabilitatea sistemului de IA;
5. Descrierea scopului preconizat al sistemului de IA;
6. Condiția sau condițiile prevăzute la articolul 6 alineatul (3) pe baza cărora sistemul de IA este considerat ca neprezentând un grad ridicat de risc;
7. Un scurt rezumat al motivelor pentru care sistemul de IA este considerat ca neprezentând un grad ridicat de risc în aplicarea procedurii prevăzute la articolul 6 alineatul (3);
8. Statutul sistemului de IA (pe piață sau în funcțiune; nu mai este pe piață/în funcțiune, rechemat);
9. Toate statele membre în care sistemul de IA a fost introdus pe piață, pus în funcțiune sau pus la dispoziție în Uniune.

Secțiunea C – Informațiile care trebuie să fie prezentate de implementatorii de sistemele de IA cu grad ridicat de risc în conformitate cu articolul 49 alineatul (3)

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la sistemele de IA cu grad ridicat de risc care se înregistrează în conformitate cu articolul 49 alineatul (3):

1. Numele/denumirea, adresa și datele de contact ale implementatorului;
2. Numele, adresa și datele de contact ale oricărei persoane care transmite informații în numele implementatorului;
3. URL-ul introducerii sistemului de IA în baza de date a UE de către furnizorul său;
4. Un rezumat al constatărilor evaluării impactului asupra drepturilor fundamentale, efectuată în conformitate cu articolul 27;
5. Un rezumat al evaluării impactului asupra protecției datelor care a fost efectuată în conformitate cu articolul 35 din Regulamentul (UE) 2016/679 sau cu articolul 27 din Directiva (UE) 2016/680, astfel cum se specifică la articolul 26 alineatul (8) din prezentul regulament, după caz.

ANEXA IX

Informațiile care trebuie să fie prezentate la înregistrarea sistemelor de IA cu grad ridicat de risc enumerate în anexa III în legătură cu testarea în condiții reale, în conformitate cu articolul 60

Se furnizează și, ulterior, se actualizează următoarele informații referitoare la testarea în condiții reale care trebuie înregistrate în conformitate cu articolul 60:

1. Un număr unic de identificare la nivelul întregii Uniuni al testării în condiții reale;
2. Numele/denumirea și datele de contact ale furnizorului sau ale potențialului furnizor și ale implementatorilor implicați în testarea în condiții reale;
3. O scurtă descriere a sistemului de IA, a scopului său preconizat și alte informații necesare pentru identificarea sistemului;
4. Un rezumat al principalelor caracteristici ale planului de testare în condiții reale;
5. Informații privind suspendarea sau încetarea testării în condiții reale.

ANEXA X

Actele legislative ale Uniunii privind sistemele informatice la scară largă în spațiul de libertate, securitate și justiție

1. Sistemul de informații Schengen

- (a) Regulamentul (UE) 2018/1860 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind utilizarea Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală (JO L 312, 7.12.2018, p. 1);
- (b) Regulamentul (UE) 2018/1861 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției de punere în aplicare a Acordului Schengen și de modificare și abrogare a Regulamentului (CE) nr. 1987/2006 (JO L 312, 7.12.2018, p. 14);
- (c) Regulamentul (UE) 2018/1862 al Parlamentului European și al Consiliului din 28 noiembrie 2018 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare și de abrogare a Deciziei 2007/533/JAI a Consiliului și de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului și a Deciziei 2010/261/UE a Comisiei (JO L 312, 7.12.2018, p. 56).

2. Sistemul de informații privind vizele

- (a) Regulamentul (UE) 2021/1133 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (UE) nr. 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 și (UE) 2019/818 în ceea ce privește stabilirea condițiilor de acces la celelalte sisteme de informații ale UE în scopuri legate de Sistemul de informații privind vizele (JO L 248, 13.7.2021, p. 1);
- (b) Regulamentul (UE) 2021/1134 al Parlamentului European și al Consiliului din 7 iulie 2021 de modificare a Regulamentelor (CE) nr. 767/2008, (CE) nr. 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 și (UE) 2019/1896 ale Parlamentului European și ale Consiliului și de abrogare a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului, în scopul reformării Sistemului de informații privind vizele (JO L 248, 13.7.2021, p. 11).

3. Eurodac

Regulamentul (UE) 2024/... al Parlamentului European și al Consiliului privind instituirea sistemului „Eurodac” pentru compararea datelor biometrice în scopul aplicării eficiente a Regulamentelor (UE) 2024/... și (UE) 2024/... ale Parlamentului European și ale Consiliului și a Directivei 2001/55/CE a Consiliului și al identificării resortisanților din țări terțe și a apatrizilor în situație de ședere ilegală și privind cererile de comparare cu datele Eurodac prezentate de autoritățile de aplicare a legii din statele membre și de Europol cu scopul de a asigura respectarea legii, de modificare a Regulamentelor (UE) 2018/1240 și (UE) 2019/818 ale Parlamentului European și ale Consiliului și de abrogare a Regulamentului (UE) nr. 603/2013 al Parlamentului European și al Consiliului⁺.

4. Sistemul de intrare/ieșire

Regulamentul (UE) 2017/2226 al Parlamentului European și al Consiliului din 30 noiembrie 2017 de instituire a Sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre, de stabilire a condițiilor de acces la EES în scopul aplicării legii și de modificare a Convenției de punere în aplicare a Acordului Schengen și a Regulamentelor (CE) nr. 767/2008 și (UE) nr. 1077/2011 (JO L 327, 9.12.2017, p. 20).

⁺ JO: a se introduce în text numărul regulamentului conținut în documentul PE-CONS 15/24 [2016/0132 (COD)] și a se introduce în nota de subsol numărul, data, titlul și referința de publicare în JO a regulamentului respectiv.

5. Sistemul european de informații și de autorizare privind călătoriile
- (a) Regulamentul (UE) 2018/1240 al Parlamentului European și al Consiliului din 12 septembrie 2018 de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 1077/2011, (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/1624 și (UE) 2017/2226 (JO L 236, 19.9.2018, p. 1);
 - (b) Regulamentul (UE) 2018/1241 al Parlamentului European și al Consiliului din 12 septembrie 2018 de modificare a Regulamentului (UE) 2016/794 în scopul instituirii Sistemului european de informații și de autorizare privind călătoriile (ETIAS) (JO L 236, 19.9.2018, p. 72).
6. Sistemul european de informații cu privire la cazierile judiciare ale resortisanților țărilor terțe și apatrizilor
- Regulamentul (UE) 2019/816 al Parlamentului European și al Consiliului din 17 aprilie 2019 de stabilire a unui sistem centralizat pentru determinarea statelor membre care dețin informații privind condamnările resortisanților țărilor terțe și ale apatrizilor (ECRIS-TCN), destinat să completeze sistemul european de informații cu privire la cazierile judiciare, și de modificare a Regulamentului (UE) 2018/1726 (JO L 135, 22.5.2019, p. 1).

7. Interoperabilitate

- (a) Regulamentul (UE) 2019/817 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul frontierelor și al vizelor și de modificare a Regulamentelor (CE) nr. 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 și (UE) 2018/1861 ale Parlamentului European și ale Consiliului și a Deciziilor 2004/512/CE și 2008/633/JAI ale Consiliului (JO L 135, 22.5.2019, p. 27);
 - (b) Regulamentul (UE) 2019/818 al Parlamentului European și al Consiliului din 20 mai 2019 privind instituirea unui cadru pentru interoperabilitatea dintre sistemele de informații ale UE în domeniul cooperării polițienești și judiciare, al azilului și al migrației și de modificare a Regulamentelor (UE) 2018/1726, (UE) 2018/1862 și (UE) 2019/816 (JO L 135, 22.5.2019, p. 85).
-

ANEXA XI

Documentația tehnică menționată la articolul 53 alineatul (1) litera (a) – documentația tehnică
pentru furnizorii de modele de IA de uz general

Secțiunea 1

Informații care trebuie furnizate de toți furnizorii de modele de IA de uz general

Documentația tehnică menționată la articolul 53 alineatul (1) litera (a) conține cel puțin următoarele informații, în funcție de dimensiunea și profilul de risc al modelului:

1. O descriere generală a modelului de IA de uz general, incluzând:
 - (a) sarcinile pe care modelul este destinat să le îndeplinească, precum și tipul și natura sistemelor de IA în care acesta poate fi integrat;
 - (b) politicile de utilizare acceptabile aplicabile;
 - (c) data eliberării și metodele de distribuție;
 - (d) arhitectura și numărul de parametri;
 - (e) modalitatea (de exemplu, text, imagine) și formatul datelor de intrare și de ieșire;
 - (f) licența.

2. O descriere detaliată a elementelor modelului menționate la punctul 1 și informații relevante privind procesul de dezvoltare, incluzând următoarele elemente:
- (a) mijloacele tehnice (de exemplu, instrucțiuni de utilizare, infrastructură, instrumente) necesare pentru integrarea modelului de IA de uz general în sistemele de IA;
 - (b) specificațiile de proiectare ale modelului și ale procesului de antrenare, inclusiv metodologiile și tehnicile de antrenare, principalele opțiuni de proiectare, inclusiv justificarea și ipotezele formulate; ce anume este proiectat să optimizeze modelul și relevanța diversilor parametri, după caz;
 - (c) informații privind datele utilizate pentru antrenare, testare și validare, după caz, inclusiv tipul și proveniența datelor și metodologiile de organizare (de exemplu, curățare, filtrare etc.), numărul de puncte de date, domeniul de aplicare și principalele caracteristici ale acestora; modul în care au fost obținute și selectate datele, precum și toate celelalte măsuri de detectare a caracterului inadecvat al surselor de date și metode de detectare a prejudecăților identificabile, după caz;
 - (d) resursele de calcul utilizate pentru antrenarea modelului (de exemplu, numărul de operații în virgulă mobilă), timpul de antrenare și alte detalii relevante legate de antrenare;
 - (e) consumul de energie cunoscut sau estimat al modelului.

În ceea ce privește litera (e), în cazul în care consumul de energie al modelului este necunoscut, consumul de energie se poate baza pe informații privind resursele de calcul utilizate.

Secțiunea 2

Informații suplimentare care trebuie furnizate de furnizorii de modele de IA de uz general cu risc sistemic

1. O descriere detaliată a strategiilor de evaluare, inclusiv a rezultatelor evaluării, pe baza protocoalelor și instrumentelor de evaluare publice disponibile sau a altor metodologii de evaluare. Strategiile de evaluare includ criterii de evaluare, indicatori și metodologia de identificare a limitărilor.
 2. După caz, o descriere detaliată a măsurilor puse în aplicare în scopul efectuării de testări contradictorii interne și/sau externe (de exemplu, testare de tipul „echipa roșie”) și de adaptări ale modelelor, inclusiv aliniere și calibrare.
 3. După caz, o descrierea detaliată a arhitecturii sistemului, care explică modul în care componentele de software se bazează una pe alta sau se susțin reciproc și se integrează în prelucrarea generală.
-

ANEXA XII

Informațiile privind transparența menționate la articolul 53 alineatul (1) litera (b)

- documentația tehnică pentru furnizorii de modele de IA de uz general
către furnizorii din aval care integrează modelul în sistemul lor de IA

Informațiile menționate la articolul 53 alineatul (1) litera (b) conțin cel puțin următoarele:

1. O descriere generală a modelului de IA de uz general, incluzând:
 - (a) sarcinile pe care modelul este destinat să le îndeplinească, precum și tipul și natura sistemelor de IA în care acesta poate fi integrat;
 - (b) politicile de utilizare acceptabile aplicabile;
 - (c) data eliberării și metodele de distribuție;
 - (d) modul în care modelul interacționează sau poate fi utilizat pentru a interacționa cu hardware-ul sau cu software-ul care nu face parte din model în sine, după caz;
 - (e) versiunile software-ului relevant legat de utilizarea modelului de IA de uz general, după caz;
 - (f) arhitectura și numărul de parametri;
 - (g) modalitatea (de exemplu, text, imagine) și formatul datelor de intrare și de ieșire;
 - (h) licența modelului.

2. O descriere a elementelor modelului și a procesului de dezvoltare a acestuia, incluzând:
- (a) mijloacele tehnice (de exemplu, instrucțiuni de utilizare, infrastructură, instrumente) necesare pentru integrarea modelului de IA de uz general în sistemele de IA;
 - (b) modalitatea (de exemplu, text, imagine) și formatul datelor de intrare și de ieșire și dimensiunea maximă a acestora (de exemplu, lungimea ferestrei de context etc.);
 - (c) informații privind datele utilizate pentru antrenare, testare și validare, după caz, inclusiv tipul și proveniența datelor și metodologiile de organizare.
-

ANEXA XIII

Criterii pentru desemnarea modelelor de IA de uz general cu risc sistemic menționate la articolul 51

Pentru a stabili dacă un model de IA de uz general are capacitățile prevăzute la articolul 51 alineatul (1) litera (a) sau un impact echivalent acestora, Comisia ia în considerare următoarele criterii:

- (a) numărul de parametri ai modelului;
- (b) calitatea sau dimensiunea setului de date, de exemplu, măsurate în tokenuri;
- (c) volumul de calcul utilizat pentru antrenarea modelului, măsurat în operații în virgulă mobilă sau indicat printr-o combinație de alte variabile, cum ar fi costul estimat al antrenării, timpul estimat necesar pentru antrenare sau consumul estimat de energie pentru antrenare;
- (d) modalitățile de intrare și de ieșire ale modelului, cum ar fi text către text (modele lingvistice de mari dimensiuni), text către imagine și multimodalitatea, și pragurile conform celui mai avansat stadiu al tehnologiei pentru determinarea capacităților cu impact ridicat pentru fiecare modalitate, precum și tipul specific de date de intrare și de ieșire (de exemplu, secvențe biologice);
- (e) valorile de referință și evaluările capacităților modelului, inclusiv luând în considerare numărul de sarcini posibile fără antrenare suplimentară, adaptabilitatea la învățarea de sarcini noi și distincte, nivelul său de autonomie și scalabilitate, instrumentele la care are acces;

- (f) dacă are un impact ridicat asupra pieței interne din cauza amplitudinii utilizării sale, care este prezumat atunci când a fost pus la dispoziția a cel puțin 10 000 de utilizatori comerciali înregistrați stabiliți în Uniune;
 - (g) numărul de utilizatori finali înregistrați.
-

POPRAVEK

Uredbe (EU) Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci)

(PE-CONS 24/1/24 REV 1, 14. junija 2024)

Uredba iz dokumenta PE-CONS 24/1/24 REV 1 se glasi:

**„UREDBA (EU) 2024/...
EVROPSKEGA PARLAMENTA IN SVETA**

z dne 13. junija 2024

**o določitvi harmoniziranih pravil o umetni inteligenci
in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013,
(EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144
ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828
(Akt o umetni inteligenci)**

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti členov 16 in 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora¹,

ob upoštevanju mnenja Evropske centralne banke²,

ob upoštevanju mnenja Odbora regij³,

v skladu z rednim zakonodajnim postopkom⁴,

¹ UL C 517, 22.12.2021, str. 56.

² UL C 115, 11.3.2022, str. 5.

³ UL C 97, 28.2.2022, str. 60.

⁴ Stališče Evropskega parlamenta z dne 13. marca 2024 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 21. maja 2024.

ob upoštevanju naslednjega:

- (1) Namen te uredbe je izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira, predvsem za razvoj, dajanje na trg, dajanje v uporabo ter za uporabo umetnointeligentnih sistemov (v nadaljnjem besedilu: sistemi UI) v Uniji, v skladu z vrednotami Unije, da bi spodbujali uvajanje na človeka osredotočene in zaupanja vredne umetne inteligence (UI) in hkrati zagotovili visoko raven varovanja zdravja, varnosti in temeljnih pravic, kot so določene v Listini Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina), vključno z demokracijo, pravno državo in varstvom okolja, za zaščito pred škodljivimi učinki sistemov UI v Uniji ter da bi podpirali inovacije. S to uredbo se zagotavlja prosti čezmejni pretok blaga in storitev, ki temeljijo na umetni inteligenci, s čimer se državam članicam preprečuje, da bi uvedle omejitve za razvoj, trženje in uporabo sistemov UI, razen če je to izrecno dovoljeno s to uredbo.
- (2) To uredbo bi bilo treba uporabljati v skladu z vrednotami Unije, zapisanimi v Listini, kar bi olajšalo varstvo fizičnih oseb, podjetij, demokracije, pravne države in varstva okolja, hkrati pa spodbujalo inovacije in zaposlovanje ter Uniji zagotovilo vodilno vlogo pri uvajanju zaupanja vredne UI.

- (3) Sisteme UI je mogoče zlahka uporabljati v številnih različnih gospodarskih in družbenih sektorjih, tudi čezmejno, in lahko enostavno krožijo po vsej Uniji. Nekatere države članice so že preučile možnost sprejetja nacionalnih predpisov, s katerimi bi zagotovile, da je UI zaupanja vredna in varna ter da se razvija in uporablja v skladu z obveznostmi glede temeljnih pravic. Različna nacionalna pravila lahko povzročijo razdrobljenost notranjega trga in zmanjšajo pravno varnost za operaterje, ki razvijajo, uvažajo ali uporabljajo sisteme UI. Zato bi bilo treba zagotoviti dosledno in visoko raven varstva po vsej Uniji, da bi dosegli zaupanja vredno UI in hkrati preprečili razlike, ki ovirajo prosti pretok, inovacije, uvajanje in uporabo sistemov UI ter z njimi povezanih proizvodov in storitev na notranjem trgu, in sicer z določitvijo enotnih obveznosti za operaterje ter zagotovitvijo enotnega varstva prevladujočih razlogov javnega interesa in pravic oseb na notranjem trgu na podlagi člena 114 Pogodbe o delovanju Evropske unije (PDEU). Kolikor ta uredba vključuje posebna pravila o varstvu posameznikov pri obdelavi osebnih podatkov v zvezi z omejitvami uporabe sistemov UI za biometrično identifikacijo na daljavo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, uporabe sistemov UI za ocene tveganja fizičnih oseb za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter uporabe sistemov UI za biometrično kategorizacijo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, je primerno, da ta uredba, kar zadeva ta posebna pravila, temelji na členu 16 PDEU. Glede na ta posebna pravila in sklicevanje na člen 16 PDEU se je primerno posvetovati z Evropskim odborom za varstvo podatkov.

- (4) UI je hitro razvijajoča se skupina tehnologij, ki prispeva k številnim gospodarskim, okoljskim in družbenim koristim v celotnem spektru panog in družbenih dejavnosti. Uporaba UI lahko z izboljšanjem napovedi, optimizacijo delovanja in dodeljevanja virov ter po meri prilagojenimi digitalnimi rešitvami, ki so na voljo posameznikom in organizacijam, zagotavlja ključne konkurenčne prednosti za podjetja ter podpira družbeno in okoljsko koristne rezultate, na primer na področju zdravstvenega varstva, kmetijstva, varnosti hrane, izobraževanja in usposabljanja, medijev, športa, kulture, upravljanja infrastrukture, energije, prometa in logistike, javnih storitev, varnosti, pravosodja, učinkovite rabe virov in energije, okoljskega spremljanja, ohranjanja in obnovitve biotske raznovrstnosti in ekosistemov ter blažitve podnebnih sprememb in prilagajanja nanje.
- (5) Hkrati lahko UI – odvisno od okoliščin v zvezi z njenim posebnim namenom, uporabo in ravno tehnološkega razvoja – povzroča tveganja ter škodi javnim interesom in temeljnim pravicam, ki jih varuje pravo Unije. Ta škoda je lahko premoženjska ali nepremoženjska, vključno s fizično, psihično, družbeno ali ekonomsko škodo.

- (6) Glede na velik vpliv, ki ga lahko ima UI na družbo, in potrebo po vzpostavitvi zaupanja je bistveno, da se UI in njen regulativni okvir razvijata v skladu z vrednotami Unije iz člena 2 Pogodbe o Evropski uniji (PEU), temeljnimi pravicami in svoboščinami, ki so zapisane v Pogodbah, in, na podlagi člena 6 PEU, v Listini. Osnovni pogoj za UI bi moral biti, da je to tehnologija, osredotočena na človeka. Morala bi biti orodje za ljudi, končni cilj pa bi moral biti povečanje njihove blaginje.
- (7) Da bi zagotovili dosledno in visoko raven zaščite javnih interesov v zvezi z zdravjem, varnostjo in temeljnimi pravicami, bi bilo treba določiti skupna pravila za visokotvegane sisteme UI. Ta pravila bi morala biti skladna z Listino, nediskriminatorna in v skladu z mednarodnimi trgovinskimi zavezami Unije. Treba bi bilo upoštevati tudi Evropsko deklaracijo o digitalnih pravicah in načelih za digitalno desetletje ter Etične smernice za zaupanja vredno umetno inteligenco strokovne skupine na visoki ravni za umetno inteligenco (AI HLEG).

- (8) Da bi spodbujali razvoj, uporabo in uvajanje UI na notranjem trgu, je torej potreben pravni okvir Unije, v katerem bodo določena harmonizirana pravila o umetni inteligenci in bo hkrati zagotovljena visoka raven zaščite javnih interesov, kot so zdravje in varnost ter varstvo temeljnih pravic, vključno z demokracijo, pravno državo in varstvom okolja, kot je priznано in zaščiteno s pravom Unije. Za doseg tega cilja bi bilo treba določiti pravila, s katerimi bo urejeno dajanje nekaterih sistemov UI na trg in v uporabo ter njihova uporaba, s čimer bo zagotovljeno nemoteno delovanje notranjega trga in bo omogočeno, da se v okviru teh sistemov izkoristi načelo prostega pretoka blaga in storitev. Ta pravila bi morala biti jasna in robustna glede varstva temeljnih pravic, morala bi podpirati nove inovativne rešitve in omogočati delovanje evropskega ekosistema javnih in zasebnih akterjev, ki ustvarjajo sisteme UI v skladu z vrednotami Unije, ter uresničevati potencial digitalne preobrazbe v vseh regijah Unije. Z določitvijo teh pravil in ukrepov v podporo inovacijam s posebnim poudarkom na malih in srednjih podjetjih (MSP), vključno s zagonskimi podjetji, ta uredba podpira cilj spodbujanja evropskega na človeka osredotočenega pristopa k umetni inteligenci in vodilnega položaja v svetu pri razvoju varne, zaupanja vredne in etične UI, kot je navedeno v sklepih Evropskega sveta⁵, in zagotavlja zaščito etičnih načel v skladu z izrecno zahtevo Evropskega parlamenta⁶.

⁵ Evropski svet, izredno zasedanje Evropskega sveta (1. in 2. oktobra 2020) – sklepi, EUCO 13/20, 2020, str. 6.

⁶ Resolucija Evropskega parlamenta z dne 20. oktobra 2020 s priporočili Komisiji o okviru etičnih vidikov umetne inteligence, robotike in sorodnih tehnologij (dok. 2020/2012(INL)).

- (9) Harmonizirana pravila, ki se uporabljajo za dajanje visokotveganih sistemov UI na trg ali v uporabo ter za njihovo uporabo, bi bilo treba določiti skladno z Uredbo (ES) št. 765/2008 Evropskega parlamenta in Sveta⁷, Sklepom št. 768/2008/ES Evropskega parlamenta in Sveta⁸ ter Uredbo (EU) 2019/1020 Evropskega parlamenta in Sveta⁹ (v nadaljnjem besedilu: novi zakonodajni okvir). Harmonizirana pravila, določena v tej uredbi, bi bilo treba uporabljati v vseh sektorjih, hkrati pa v skladu z novim zakonodajnim okvirom ne bi smela posegati v veljavno pravo Unije, zlasti pravo o varstvu podatkov, varstvu potrošnikov, temeljnih pravicah, zaposlovanju in varstvu delavcev ter varnosti proizvodov, ki ga ta uredba dopolnjuje. Posledično ostanejo nespremenjeni in se v celoti uporabljajo vse pravice in pravna sredstva, ki jih takšno pravo Unije zagotavlja potrošnikom in drugim osebam, na katere bi lahko sistemi UI negativno vplivali, tudi v zvezi z nadomestilom morebitne škode na podlagi Direktive Sveta 85/374/EGS¹⁰.

⁷ Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).

⁸ Sklep št. 768/2008/ES Evropskega parlamenta in Sveta z dne 9. julija 2008 o skupnem okviru za trženje proizvodov in razveljavitvi Sklepa Sveta 93/465/EGS (UL L 218, 13.8.2008, str. 82).

⁹ Uredba (EU) 2019/1020 Evropskega parlamenta in Sveta z dne 20. junija 2019 o nadzoru trga in skladnosti proizvodov ter spremembi Direktive 2004/42/ES in uredb (ES) št. 765/2008 in (EU) št. 305/2011 (UL L 169, 25.6.2019, str. 1).

¹⁰ Direktiva Sveta 85/374/EGS z dne 25. julija 1985 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako (UL L 210, 7.8.1985, str. 29).

Poleg tega ta uredba v okviru zaposlovanja in zaščite delavcev ne bi smela vplivati na pravo Unije o socialni politiki in nacionalno delovno pravo, ki je skladno s pravom Unije, v zvezi z zaposlovanjem in delovnimi pogoji, vključno z zdravjem in varnostjo pri delu ter razmerjem med delodajalci in delavci. Tudi ne bi smela vplivati na uveljavljanje temeljnih pravic, ki so priznane v državah članicah in na ravni Unije, vključno s pravico do stavke ali drugih ukrepov, zajetih v specifičnih sistemih odnosov med delodajalci in delojemalci v posameznih državah članicah, ter na pravico do pogajanj, sklepanja in izvrševanja kolektivnih pogodb ali do kolektivnih ukrepov v skladu z nacionalnim pravom. Ta uredba ne bi smela vplivati na določbe za izboljšanje delovnih pogojev pri platformnem delu iz direktive Evropskega parlamenta in Sveta o izboljšanju delovnih pogojev pri platformnem delu. Namen te uredbe je tudi okrepiti učinkovitost takih obstoječih pravic in pravnih sredstev z določitvijo posebnih zahtev in obveznosti, tudi glede preglednosti, tehnične dokumentacije in vodenja evidenc sistemov UI. Poleg tega bi bilo treba obveznosti, naložene različnim operaterjem, vključenim v verigo vrednosti UI na podlagi te uredbe, uporabljati brez poseganja v nacionalno pravo, ki je skladno s pravom Unije in katerega učinek je omejitev uporabe nekaterih sistemov UI, kadar tako pravo ne spada na področje uporabe te uredbe ali je namenjeno uresničevanju legitimnih ciljev v javnem interesu, ki niso cilji iz te uredbe. Ta uredba na primer ne bi smela vplivati na nacionalno delovno pravo in pravo o varstvu mladoletnikov, tj. oseb, mlajših od 18 let, ob upoštevanju Splošne pripombe št. 25 KZNOP (2021) o otrokovih pravicah v zvezi z digitalnim okoljem, če se to pravo ne nanaša posebej na sisteme UI in je namenjeno uresničevanju drugih legitimnih ciljev v javnem interesu.

- (10) Temeljna pravica do varstva osebnih podatkov je zajamčena zlasti z uredbama (EU) 2016/679¹¹ in (EU) 2018/1725¹² Evropskega parlamenta in Sveta ter Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta¹³. Direktiva 2002/58/ES Evropskega parlamenta in Sveta¹⁴ poleg tega varuje zasebno življenje in zaupnost komunikacij, vključno z zagotavljanjem pogojev za shranjevanje osebnih in neosebnih podatkov na terminalski opremi in za dostop do teh podatkov z nje. Navedeni pravni akti Unije so podlaga za vzdržno in odgovorno obdelavo podatkov, tudi kadar nabori podatkov vključujejo kombinacijo osebnih in neosebnih podatkov. Namen te uredbe ni vplivati na uporabo veljavnega prava Unije, ki ureja obdelavo osebnih podatkov, med drugim tudi ne na naloge in pooblastila neodvisnih nadzornih organov, pristojnih za spremljanje skladnosti s temi instrumenti.

¹¹ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

¹² Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

¹³ Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89).

¹⁴ Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (UL L 201, 31.7.2002, str. 37).

Uredba tudi ne vpliva na obveznosti ponudnikov in uvajalcev sistemov UI v njihovi vlogi upravljavcev ali obdelovalcev podatkov, ki izhaja iz prava Unije ali nacionalnega prava o varstvu osebnih podatkov, če zasnova, razvoj ali uporaba sistemov UI vključuje obdelavo osebnih podatkov. Prav tako je treba pojasniti, da posamezniki, na katere se nanašajo osebni podatki, še naprej uživajo vse pravice in jamstva, ki jim jih podeljuje tovrstno pravo Unije, tudi pravice, povezane izključno z avtomatiziranim sprejemanjem posameznih odločitev, vključno z oblikovanjem profilov. Harmonizirana pravila za dajanje sistemov UI na trg ali v uporabo ter za njihovo uporabo, ki so določena na podlagi te uredbe, bi morala olajšati učinkovito izvajanje in omogočiti uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki, in drugih pravnih sredstev, zagotovljenih na podlagi prava Unije o varstvu osebnih podatkov in drugih temeljnih pravic.

- (11) Ta uredba ne bi smela posegati v določbe o odgovornosti ponudnikov posredniških storitev iz Uredbe (EU) 2022/2065 Evropskega parlamenta in Sveta¹⁵.

¹⁵ Uredba (EU) 2022/2065 Evropskega parlamenta in Sveta z dne 19. oktobra 2022 o enotnem trgu digitalnih storitev in spremembi Direktive 2000/31/ES (Akt o digitalnih storitvah) (UL L 277, 27.10.2022, str. 1).

- (12) Pojem „sistem UI“ v tej uredbi bi moral biti jasno opredeljen in tesno usklajen z delom mednarodnih organizacij, ki se ukvarjajo z UI, da bi zagotovili pravno varnost, olajšali mednarodno zbliževanje in široko sprejemanje ter hkrati zagotovili prožnost, ki bo omogočala prilagajanje hitremu tehnološkemu razvoju na tem področju. Poleg tega bi morala opredelitev temeljiti na ključnih značilnostih sistemov UI, po katerih se razlikuje od enostavnejših tradicionalnih sistemov programske opreme ali programskih pristopov, in ne bi smela vključevati sistemov, ki temeljijo na pravilih, ki jih za samodejno izvajanje operacij opredelijo izključno fizične osebe. Ključna značilnost sistemov UI je njihova sposobnost sklepanja. Ta sposobnost sklepanja se nanaša na proces pridobivanja izhodnih podatkov, kot so napovedi, vsebina, priporočila ali odločitve, ki lahko vplivajo na fizično in virtualno okolje, ter na sposobnost sistemov UI, da izpeljejo modele ali algoritme ali oboje iz vhodnih vrednosti ali podatkov. Tehnike, ki omogočajo sklepanje pri vzpostavljanju sistema UI, vključujejo pristope strojnega učenja, ki se tega, kako doseči določene cilje, učijo iz podatkov, ter pristope, ki temeljijo na logiki in znanju ter izhajajo iz kodiranega znanja ali simbolične predstavitve naloge, ki jo je treba rešiti. Zmogljivost sistema UI za sklepanje presega osnovno obdelavo podatkov z omogočanjem učenja, prihajanja do zaključkov ali modeliranja. Izraz „temelječ na napravah“ se nanaša na dejstvo, da sisteme UI poganjajo stroji.

Sklicevanje na eksplicitne ali implicitne cilje poudarja, da lahko sistemi UI delujejo v skladu z eksplicitnimi ali implicitnimi cilji. Cilji sistema UI se lahko v posebnih okoliščinah razlikujejo od predvidenega namena sistema UI. Za namene te uredbe bi bilo treba okolja razumeti kot kontekste, v katerih delujejo sistemi UI, medtem ko izhodni podatki, ki jih ustvari sistem UI, odražajo različne funkcije, ki jih opravljajo sistemi UI, in vključujejo napovedi, vsebine, priporočila ali odločitve. Sistemi UI so zasnovani tako, da delujejo z različnimi stopnjami avtonomije, kar pomeni, da so do neke mere neodvisni od človeškega sodelovanja in zmožni delovati brez človeškega posredovanja. Prilagodljivost, ki bi jo sistem UI lahko pokazal po uvedbi, se nanaša na sposobnosti samoučenja, ki omogočajo, da se sistem med uporabo spremeni. Sistemi UI se lahko uporabljajo samostojno ali kot komponenta določenega proizvoda, ne glede na to, ali je sistem fizično integriran v proizvod (vgrajen) ali služi funkcionalnosti proizvoda, ne da bi bil vanj integriran (nevgrajen).

- (13) Pojem „uvajalec“ iz te uredbe bi bilo treba razlagati kot vsako fizično ali pravno osebo, vključno z javnim organom, agencijo ali drugim telesom, ki uporablja sistem UI pod svojo pristojnostjo, razen kadar se sistem UI uporablja v okviru osebne nepoklicne dejavnosti. Glede na vrsto sistema UI lahko uporaba sistema vpliva na osebe, ki niso uvajalec.
- (14) Pojem „biometrični podatki“, ki se uporablja v tej uredbi, bi bilo treba razlagati glede na pojem biometričnih podatkov, kot je opredeljen v členu 4, točka 14, Uredbe (EU) 2016/679, členu 3, točka 18, Uredbe (EU) 2018/1725 in členu 3, točka 13, Direktive (EU) 2016/680. Biometrični podatki lahko omogočijo avtentikacijo, identifikacijo ali kategorizacijo fizičnih oseb in prepoznavanje njihovih čustev.
- (15) Pojem „biometrična identifikacija“ iz te uredbe bi bilo treba opredeliti kot avtomatizirano prepoznavanje fizičnih, fizioloških in vedenjskih človeških značilnosti, kot so obraz, gibanje oči, izrazi obraza, oblika telesa, glas, govor, hoja, drža, srčni utrip, krvni tlak, vonj in značilnosti tipkanja, za namene preverjanja identitete posameznika s primerjavo biometričnih podatkov tega posameznika s shranjenimi biometričnimi podatki posameznikov v referenčni podatkovni zbirki ne glede na to, ali je posameznik v to privolil ali ne. To izključuje sisteme UI za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja, in potrditi identiteto fizične osebe izključno z namenom dostopa do storitve, odklepanja naprave ali varnostnega dostopa do prostorov.

- (16) Pojem „biometrična kategorizacija“ iz te uredbe bi bilo treba opredeliti kot razvrstitev fizičnih oseb v posebne kategorije na podlagi njihovih biometričnih podatkov. Takšne posebne kategorije se lahko nanašajo na vidike, kot so spol, starost, barva las, barva oči, tetovaže, vedenjske ali osebnostne lastnosti, jezik, vera, pripadnost narodnostni manjšini, spolna ali politična usmerjenost. To ne vključuje sistemov za biometrično kategorizacijo, ki so izključno pomožni element, neločljivo povezan z drugo komercialno storitvijo, kar pomeni, da tega elementa iz objektivnih tehničnih razlogov ni mogoče uporabiti brez glavne storitve, njegova vključitev ali funkcionalnost pa ni sredstvo za izogibanje uporabi pravil iz te uredbe. Na primer, filtri za kategorizacijo obraznih ali telesnih značilnosti, ki se uporabljajo na spletnih tržnicah, bi lahko bili takšen pomožni element, saj se lahko uporabljajo le v zvezi z glavno storitvijo, ki je prodaja izdelka na način, da se potrošniku omogoči, da si ogleda prikaz izdelka sam, in se mu pomaga pri sprejemanju odločitve o nakupu. Filtre, ki se uporabljajo na spletnih storitvah družbenih omrežij in s katerimi se kategorizirajo obrazne funkcije ali funkcije telesa, da lahko uporabniki dodajajo ali spreminjajo slike ali videoposnetke, bi prav tako lahko šteli za pomožno funkcijo, saj takega filtra ni mogoče uporabljati brez glavne storitve, tj. storitev družbenih omrežij, ki vključuje izmenjavo vsebin na spletu.

- (17) Pojem „sistem za biometrično identifikacijo na daljavo“ iz te uredbe bi bilo treba opredeliti funkcionalno kot sistem UI, namenjen identifikaciji fizičnih oseb brez njihovega dejavnega sodelovanja, običajno na daljavo, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke, ne glede na uporabljeno tehnologijo, procese ali vrste biometričnih podatkov. Takšni sistemi za biometrično identifikacijo na daljavo se običajno uporabljajo za hkratno zaznavanje več oseb ali njihovega vedenja, da se bistveno olajša identifikacija fizičnih oseb brez njihovega dejavnega sodelovanja. To izključuje sisteme UI za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja, in potrditi identiteto fizične osebe izključno z namenom dostopa do storitve, odklepanja naprave ali varnostnega dostopa do prostorov. Ta izključitev je utemeljena z dejstvom, da bodo imeli taki sistemi verjetno manjši vpliv na temeljne pravice fizičnih oseb v primerjavi s sistemi za biometrično identifikacijo na daljavo, ki se lahko uporabljajo za obdelavo biometričnih podatkov velikega števila oseb brez njihovega dejavnega sodelovanja. Pri sistemih „v realnem času“ se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo takoj ali skoraj takoj, v vsakem primeru pa brez večje zamude. V zvezi s tem ne bi smelo biti prostora za izogibanje pravilom te uredbe o uporabi zadevnih sistemov UI „v realnem času“, saj je predvidena možnost manjših zamud. Sistemi „v realnem času“ vključujejo uporabo gradiva „v živo“ ali „skoraj v živo“, kot je videoposnetek, ki ga ustvari kamera ali druga naprava s podobno funkcionalnostjo. Pri „naknadnih“ sistemih so bili biometrični podatki že zajeti, primerjava in identifikacija pa se izvedeta šele po daljšem času. To vključuje gradivo, kot so slike ali videoposnetki, ki jih ustvarjajo kamere CCTV ali zasebne naprave, ki je bilo ustvarjeno pred uporabo sistema v zvezi z zadevnimi fizičnimi osebami.

- (18) Pojem „sistem za prepoznavanje čustev“ iz te uredbe bi bilo treba opredeliti kot sistem UI za prepoznavanje čustev ali namer ali za sklepanje o čustvih ali namerah fizičnih oseb na podlagi njihovih biometričnih podatkov. Pojem se nanaša na čustva ali namere, kot so sreča, žalost, jeza, presenečenje, ogorčenje, zadrega, navdušenje, osramočenost, zaničevanje, zadovoljstvo in zabavanje. Ne vključuje fizičnih stanj, kot sta bolečina ali utrujenost, na primer vključno s sistemi, ki se uporabljajo za odkrivanje stanja utrujenosti poklicnih pilotov ali voznikov za namene preprečevanja nesreč. To tudi ne vključuje zgolj odkrivanja lahko vidnih izrazov, gest ali gibov, razen če se uporabljajo za prepoznavanje čustev ali sklepanje o njih. Ti izrazi so lahko osnovni obrazni izrazi, kot je namrščenost ali nasmeh, ali geste, kot je premikanje dlani, rok ali glave, ali značilnosti glasu osebe, kot je povzdignjen glas ali šepetanje.

- (19) Za namene te uredbe bi bilo treba pojem javno dostopnega prostora razumeti kot vsak fizični prostor, ki je dostopen nedoločenemu številu fizičnih oseb, ne glede na to, ali je ta prostor v zasebni ali javni lasti, in ne glede na dejavnost, za katero se ta prostor uporablja, denimo za komercialno, na primer trgovine, restavracije, kavarne; storitveno, na primer banke, poklicne dejavnosti, gostinske ali nastanitvene dejavnosti; športno, na primer bazeni, telovadnice, stadioni; prevozno, na primer avtobusne postaje, postaje podzemne železnice in železniške postaje, letališča, prevozna sredstva; razvedrilno, na primer kinematografi, gledališča, muzeji, koncertne in konferenčne dvorane; prostočasno ali drugo dejavnost, na primer javne ceste in trgi, parki, gozdovi, igrišča. Prostor bi bilo treba tudi razvrstiti kot javno dostopen, če za dostop ne glede na morebitne omejitve zmogljivosti ali varnostne omejitve veljajo nekateri vnaprej določeni pogoji, ki jih lahko izpolni nedoločeno število oseb, kot je nakup vstopnice ali vozovnice, predhodna registracija ali določena starost. Nasprotno pa se prostor ne bi smel šteti za javno dostopnega, če je dostop omejen na določene in opredeljene fizične osebe bodisi na podlagi prava Unije bodisi na podlagi nacionalnega prava, ki se neposredno nanaša na javno varnost ali varovanje, ali če se oseba, ki ima za ta prostor ustrezna pooblastila, glede tega jasno opredeli. Dejanska možnost samega dostopa, kot so odklenjena vrata, odprta vrata v ograji, ne pomeni, da je prostor javno dostopen, če obstajajo znaki ali okoliščine, ki kažejo na nasprotno, kot so znaki, ki prepovedujejo ali omejujejo dostop. Prostori podjetij in tovarn ter pisarne in delovni prostori, do katerih naj bi dostopali samo ustrezni zaposleni in ponudniki storitev, so prostori, ki niso javno dostopni. Javno dostopni prostori ne bi smeli vključevati zaporov ali območij mejne kontrole. Nekateri drugi prostori lahko zajemajo tako javno dostopne kot javno nedostopne prostore, kot je hodnik ali veža zasebne stanovanjske zgradbe, prek katere se dostopa do zdravniške pisarne, ali letališče. Spletni prostori niso zajeti, saj niso fizični prostori. Ali je določen prostor dostopen javnosti ali ne, pa je treba ugotoviti za vsak primer posebej, ob upoštevanju posebnosti posamezne dane situacije.

- (20) Da bi dosegli največje koristi sistemov UI in hkrati zaščitili temeljne pravice, zdravje in varnost ter omogočili demokratični nadzor, bi morala pismenost na področju UI ponudnikom, uvajalcem in osebam, na katere vpliva sistem UI, omogočiti razumevanje potrebnih pojmov za sprejemanje informiranih odločitev v zvezi s sistemi UI. Ti pojmi se lahko razlikujejo glede na zadevni kontekst in lahko vključujejo razumevanje pravilne uporabe tehničnih elementov v razvojni fazi sistema UI, ukrepe, ki jih je treba uporabiti med njegovo uporabo, ustrezne načine za razlago izhodnih podatkov sistema UI in, v primeru oseb, na katere vpliva sistem UI, znanje, potrebno za razumevanje, kako bodo odločitve, sprejete s pomočjo UI vplivale nanje. V okviru uporabe te uredbe bi morala pismenost na področju UI vsem zadevnim akterjem v verigi vrednosti UI zagotoviti vpoglede, potrebne za zagotovitev ustrezne skladnosti s to uredbo in njenega pravilnega izvrševanja. Poleg tega bi lahko široko izvajanje ukrepov za pismenost na področju UI in uvedba ustreznih nadaljnjih ukrepov prispevala k izboljšanju delovnih pogojev ter nazadnje podprla konsolidacijo in inovacijsko pot zaupanja vredne UI v Uniji. Evropski odbor za umetno inteligenco (v nadaljnjem besedilu: Odbor) bi moral podpirati Komisijo pri spodbujanju orodij za pismenost na področju UI, ozaveščenosti javnosti in razumevanja koristi, tveganj, zaščitnih ukrepov, pravic in obveznosti v zvezi z uporabo sistemov UI. Komisija in države članice bi morale v sodelovanju z ustreznimi deležniki olajšati pripravo prostovoljnih kodeksov ravnanja za izboljšanje pismenosti na področju UI med osebami, ki se ukvarjajo z razvojem, delovanjem in uporabo UI.

- (21) Za zagotovitev enakih konkurenčnih pogojev ter učinkovitega varstva pravic in svoboščin posameznikov po vsej Uniji bi se morala pravila iz te uredbe nediskriminatorno uporabljati za ponudnike sistemov UI, ne glede na to, ali imajo sedež v Uniji ali v tretji državi, in za uvajalce sistemov UI s sedežem v Uniji.
- (22) Zaradi svoje digitalne narave bi morali nekateri sistemi UI spadati na področje uporabe te uredbe, tudi če niso dani na trg ali v uporabo oziroma se ne uporabljajo v Uniji. To velja na primer za operaterja s sedežem v Uniji, ki določene storitve naroča pri operaterju s sedežem v tretji državi v zvezi z dejavnostjo, ki jo bo izvajal sistem UI, ki bi bil opredeljen kot visokotvegani sistem. V teh okoliščinah bi lahko sistem UI, ki ga operater uporablja v tretji državi, obdeloval podatke, ki se zakonito zbirajo v Uniji in prenašajo iz nje, ter naročniku v Uniji zagotovil izhodne podatke navedenega sistema UI, ki izhajajo iz te obdelave, ne da bi bil ta sistem UI dan na trg ali v uporabo oziroma bi se uporabljal v Uniji. Da bi preprečili izogibanje določbam te uredbe in zagotovili učinkovito varstvo fizičnih oseb v Uniji, bi se morala ta uredba uporabljati tudi za ponudnike in uvajalce sistemov UI s sedežem v tretji državi, če so izhodni podatki, ki jih ti sistemi ustvarijo, namenjeni uporabi v Uniji.

Kljub temu pa se zaradi upoštevanja obstoječih ureditev in posebnih potreb po prihodnjem sodelovanju s tujimi partnerji, s katerimi se izmenjujejo informacije in dokazi, ta uredba ne bi smela uporabljati za javne organe tretje države in mednarodne organizacije, kadar delujejo v okviru sodelovanja ali mednarodnih sporazumov, sklenjenih na ravni Unije ali nacionalni ravni za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pravosodnega sodelovanja z Unijo ali državami članicami, pod pogojem, da zadevna tretja država ali mednarodne organizacije zagotovijo ustrezne zaščitne ukrepe v zvezi z varstvom temeljnih pravic in svoboščin posameznikov. To lahko po potrebi zajema dejavnosti subjektov, ki so jim tretje države zaupale izvajanje posebnih nalog v podporo takemu sodelovanju na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter pri pravosodnem sodelovanju. Takšni okviri za sodelovanje ali sporazumi so bili vzpostavljeni dvostransko med državami članicami in tretjimi državami ali med Evropsko unijo, Europolom in drugimi agencijami Unije ter tretjimi državami in mednarodnimi organizacijami. Organi, pristojni za nadzor organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter pravosodnih organov v skladu s to uredbo, bi morali oceniti, ali navedeni okviri za sodelovanje ali mednarodni sporazumi vključujejo ustrezne zaščitne ukrepe v zvezi z varstvom temeljnih pravic in svoboščin posameznikov. Nacionalni organi prejemniki ter institucije, organi, uradi in agencije Unije, ki uporabljajo take izhodne podatke v Uniji, so še naprej odgovorni za zagotavljanje, da je njihova uporaba skladna s pravom Unije. Ko se ti mednarodni sporazumi revidirajo ali se v prihodnosti sklenejo novi, bi si morale pogodbenice kar najbolj prizadevati za njihovo uskladitev z zahtevami iz te uredbe.

- (23) To uredbo bilo treba uporabljati tudi za institucije, organe, urade in agencije Unije, kadar delujejo kot ponudniki ali uvajalci sistema UI.

- (24) Če in kolikor so sistemi UI s spremembami ali brez njih dani na trg ali v uporabo oziroma se uporabljajo za vojaške ali obrambne namene ali namene nacionalne varnosti, bi morali biti izključeni iz področja uporabe te uredbe ne glede na to, katera vrsta subjekta izvaja te dejavnosti, tj. ali gre za javni ali zasebni subjekt. Kar zadeva vojaške in obrambne namene, je taka izključitev utemeljena tako s členom 4(2) PEU kot tudi s posebnostmi obrambne politike držav članic in skupne obrambne politike Unije iz naslova V, poglavje 2, PEU, za katere velja mednarodno javno pravo, ki je zato ustrežnejši pravni okvir za ureditev sistemov UI v kontekstu uporabe smrtonosne sile in drugih sistemov UI v kontekstu vojaških in obrambnih dejavnosti. Kar zadeva namene nacionalne varnosti, izključitev upravičuje tako dejstvo, da nacionalna varnost ostaja v izključni pristojnosti držav članic v skladu s členom 4(2) PEU, kot tudi posebna narava in operativne potrebe dejavnosti nacionalne varnosti ter posebna nacionalna pravila, ki se za te dejavnosti uporabljajo. Če pa se sistem UI, ki je bil razvit, dan na trg ali v uporabo oziroma se uporablja v vojaške ali obrambne namene ali namene nacionalne varnosti, začasno ali stalno uporablja za druge namene (na primer civilne ali humanitarne namene, namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali namene javne varnosti), bi tak sistem spadal na področje uporabe te uredbe. V tem primeru bi moral subjekt, ki sistem UI uporablja za namene, ki niso vojaški ali obrambni nameni ali nameni nacionalne varnosti, zagotoviti skladnost sistema UI s to uredbo, razen če je sistem že skladen s to uredbo. Sistemi UI, ki so dani na trg ali v uporabo za izključene namene, tj. vojaške, obrambne namene ali namene nacionalne varnosti, in enega ali več neizključenih namenov, kot so civilni nameni ali nameni preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, spadajo na področje uporabe te uredbe, njihovi ponudniki pa bi morali zagotoviti skladnost s to uredbo. V teh primerih dejstvo, da sistem UI lahko spada na področje uporabe te uredbe, ne bi smelo vplivati na možnost subjektov, ki izvajajo nacionalne varnostne, obrambne in vojaške dejavnosti (ne glede na vrsto teh subjektov), da uporabljajo sisteme UI za namene nacionalne varnosti, vojaške in obrambne namene, katerih uporaba je izključena iz področja uporabe te uredbe. Sistem UI, dan na trg za civilne namene ali namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ki se uporablja s spremembami ali brez njih za vojaške in obrambne namene ali namene nacionalne varnosti, ne bi smel spadati na področje uporabe te uredbe, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

- (25) S to uredbo bi bilo treba podpirati inovacije in spoštovati svobodo znanosti ter z njo ne bi smeli ogrožati raziskovalnih in razvojnih dejavnosti. Zato je treba iz njenega področja uporabe izključiti sisteme in modele UI, ki so bili posebej razviti in dani v uporabo izključno za znanstvene raziskave in razvoj. Poleg tega je treba zagotoviti, da ta uredba ne vpliva kako drugače na znanstvene raziskave in razvoj sistemov ali modelov UI, preden se dajo na trg ali v uporabo. Tudi kar zadeva v proizvode usmerjene raziskave, testiranje in razvoj sistemov ali modelov UI, se določbe te uredbe ne bi smele uporabljati pred dajanjem teh sistemov in modelov v uporabo ali na trg. Ta izključitev pa ne posega v obveznost skladnosti s to uredbo, če je sistem UI, ki spada na področje uporabe te uredbe, dan na trg ali v uporabo kot rezultat take raziskovalne in razvojne dejavnosti, ter v uporabo določb o regulativnih peskovnikih za UI in testiranju v realnih razmerah. Poleg tega bi morale brez poseganja v izključitev sistemov UI, ki so posebej razviti in dani v uporabo izključno za namene znanstvenih raziskav in razvoja, za vse druge sisteme UI, ki se lahko uporabljajo za izvajanje kakršnih koli raziskovalnih in razvojnih dejavnosti, še naprej veljati določbe te uredbe. V vsakem primeru bi bilo treba vsakršno raziskovalno in razvojno dejavnost izvajati v skladu s priznanimi etičnimi in strokovnimi standardi za znanstvene raziskave ter v skladu z veljavnim pravom Unije.

- (26) Za uvedbo sorazmernega in učinkovitega sklopa zavezujočih pravil za sisteme UI bi bilo treba upoštevati jasno opredeljen pristop, ki temelji na tveganju. Ta pristop bi moral vrsto in vsebino takih pravil prilagoditi intenzivnosti in obsegu tveganj, ki jih lahko ustvarijo sistemi UI. Zato je treba prepovedati nekatere nesprejemljive prakse UI, določiti zahteve za visokotvegane sisteme UI in obveznosti za zadevne operaterje ter določiti obveznosti glede preglednosti za nekatere sisteme UI.
- (27) Čeprav je pristop, ki temelji na tveganju, podlaga za sorazmeren in učinkovit sklop zavezujočih pravil, je pomembno opozoriti na Etične smernice za zaupanja vredno umetno inteligenco iz leta 2019, ki jih je razvila neodvisna strokovna skupina na visoki ravni za umetno inteligenco (AI HLEG), ki jo je imenovala Komisija. V teh smernicah je AI HLEG razvila sedem nezavezujočih etičnih načel za UI, ki naj bi pomagala zagotoviti, da je UI zaupanja vredna in etično zanesljiva. Teh sedem načel vključuje človeško delovanje in nadzor, tehnično robustnost in varnost, zasebnost in upravljanje podatkov, preglednost, raznolikost, nediskriminacijo in pravičnost ter družbeno in okoljsko blaginjo in odgovornost. Brez poseganja v pravno zavezujoče zahteve te uredbe in katerega koli drugega veljavnega prava Unije te smernice prispevajo k oblikovanju skladne, zaupanja vredne in na človeka osredotočene UI v skladu z Listino in vrednotami, na katerih temelji Unija. V skladu s smernicami AI HLEG človeško delovanje in nadzor pomeni, da se sistemi UI razvijajo in uporabljajo kot orodje, ki služi ljudem, spoštuje človeško dostojanstvo in osebno avtonomijo ter deluje tako, da ga ljudje lahko ustrezno upravljajo in nadzorujejo.

Tehnična robustnost in varnost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki omogoča robustnost v primeru težav in odpornost proti poskusom spremembe uporabe ali učinkovitosti sistema UI, ki bi lahko tretjim osebam omogočila nezakonito uporabo, in čim bolj zmanjša nenamerno škodo. Zasebnost in upravljanje podatkov pomeni, da se sistemi UI razvijajo in uporabljajo v skladu s pravili o zasebnosti in varstvu podatkov, hkrati pa obdelujejo podatke, ki izpolnjujejo visoke standarde v smislu kakovosti in celovitosti. Preglednost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki omogoča ustrezno sledljivost in razložljivost, obenem pa so ljudje seznanjeni s tem, da komunicirajo ali da so v stiku s sistemom UI, uvajalci so ustrezno obveščeni o zmogljivostih in omejitvah zadevnega sistema UI, osebe, na katere vpliva sistem UI, pa o svojih pravicah. Raznolikost, nediskriminacija in pravičnost pomeni, da se sistemi UI razvijajo in uporabljajo na način, ki vključuje različne akterje in spodbuja enakopraven dostop, enakost spolov in kulturno raznolikost, hkrati pa se preprečujejo diskriminatorni učinki in nepravilni predsodki, ki jih pravo Unije ali držav članic prepoveduje. Družbena in okoljska blaginja pomeni, da se sistemi UI razvijajo in uporabljajo na trajnosten in okolju prijazen način ter v korist vseh ljudi, hkrati pa se spremljajo in ocenjujejo dolgoročni vplivi na posameznika, družbo in demokracijo. Ta načela bi bilo treba uporabljati tudi pri zasnovi in uporabi modelov UI, kadar je mogoče. V vsakem primeru bi morala biti podlaga za pripravo kodeksov ravnanja na podlagi te uredbe. Vsi deležniki, vključno z industrijo, akademskimi krogi, civilno družbo in organizacijami za standardizacijo, naj ustrezno upoštevajo etična načela za razvoj prostovoljnih najboljših praks in standardov.

- (28) Poleg številnih koristnih uporab UI jo je mogoče tudi zlorabiti, tako da bi nastala nova in močna orodja za prakse manipulacije, izkoriščanja in družbenega nadzora. Take prakse so še posebej škodljive in zlonamerne in bi jih bilo treba prepovedati, ker so v nasprotju z vrednotami Unije glede spoštovanja človekovega dostojanstva, svobode, enakosti, demokracije in pravne države ter temeljnimi pravicami, določenimi v Listini, vključno s pravico do nediskriminacije, varstva podatkov in zasebnosti ter pravicami otroka.

- (29) Z UI omogočene manipulativne tehnike se lahko uporabljajo za napeljevanje oseb k neželenemu vedenju ali za njihovo zavajanje, tako da se jih spodbuja k odločitvam na način, ki spodkopava in ovira njihovo avtonomijo, odločanje in svobodno izbiro. Dajanje na trg, dajanje v uporabo ali uporaba nekaterih sistemov UI s ciljem ali učinkom bistvenega izkrivljanja človeškega vedenja, pri čemer je verjetno, da bo nastala znatna škoda, zlasti z dovolj pomembnimi škodljivimi učinki na telesno ali duševno zdravje ali finančne interese, je še posebej nevarno oziroma nevarna in bi ga oziroma jo bilo zato treba prepovedati. Takšni sistemi UI uporabljajo subliminalne komponente, kot so zvočni, slikovni ali video dražljaji, ki jih osebe ne morejo zaznati, ker ti dražljaji presegajo človekovo dožemanje, ali druge manipulativne ali zavajajoče tehnike, ki spodkopavajo ali ovirajo posameznikovo avtonomijo, odločanje ali svobodno izbiro na načine, da se ljudje ne zavedajo teh tehnik ali pa, kadar se jih zavedajo, so kljub temu lahko zavedeni ali jih ne morejo nadzorovati ali se jim upreti. To bi bilo na primer mogoče olajšati z vmesniki stroj-možgani ali virtualno resničnostjo, saj omogočajo višjo stopnjo nadzora nad tem, kateri dražljaji so predstavljeni osebam, če lahko bistveno izkrivljajo njihovo vedenje na znatno škodljiv način. Sistemi UI lahko tudi sicer izkoriščajo šibke točke določene osebe ali skupine oseb zaradi njihove starosti, invalidnosti v smislu Direktive (EU) 2019/882 Evropskega parlamenta in Sveta¹⁶ ali posebnih socialnih ali gospodarskih razmer, zaradi katerih so te osebe verjetno bolj izpostavljene izkoriščanju, na primer osebe, ki živijo v skrajni revščini, ter etnične ali verske manjšine.

¹⁶ Direktiva (EU) 2019/882 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o zahtevah glede dostopnosti za proizvode in storitve (UL L 151, 7.6.2019, str. 70).

Takšni sistemi UI se lahko dajo na trg ali v uporabo oziroma se uporabljajo s ciljem ali učinkom bistvenega izkrivljanja vedenja osebe, in sicer na način, ki tej ali drugi osebi ali skupinam oseb povzroči znatno škodo, vključno s škodo, ki se lahko sčasoma nakopiči, ali za katerega obstaja razumna verjetnost, da jo bo povzročil, zato bi morali biti prepovedani. Morda ni mogoče domnevati, da obstaja namen izkrivljanja vedenja, kadar je izkrivljanje posledica dejavnikov zunaj sistema UI, na katere ponudnik ali uvajalec ne more vplivati, in sicer dejavnikov, ki jih ni mogoče razumno predvideti in jih zato ponudnik ali uvajalec sistema UI ne more zmanjšati. V vsakem primeru ni potrebno, da ima ponudnik ali uvajalec namen povzročiti znatno škodo, če takšna škoda izhaja iz manipulativnih ali izkoriščevalskih praks, ki jih omogoča UI. Prepovedi takih praks UI dopolnjujejo določbe Direktive 2005/29/ES Evropskega parlamenta in Sveta¹⁷, zlasti v smislu, da so nepoštenne poslovne prakse, ki potrošnikom povzročajo gospodarsko ali finančno škodo, prepovedane v vseh okoliščinah, ne glede na to, ali se izvajajo prek sistemov UI ali kako drugače. Prepoved manipulativnih in izkoriščevalskih praks iz te uredbe ne bi smela vplivati na zakonite prakse v okviru zdravljenja, kot je psihološko zdravljenje duševne bolezni ali telesna rehabilitacija, kadar se te prakse izvajajo v skladu z veljavnimi pravnimi medicinskimi standardi in zakonodajo, kot na primer izrecna privolitev posameznikov ali njihovih zakonitih zastopnikov. Poleg tega se običajne in zakonite poslovne prakse, na primer na področju oglaševanja, ki so v skladu z veljavnim pravom, same po sebi ne bi smele šteti za škodljive manipulativne z UI omogočene prakse.

¹⁷ Direktiva Evropskega parlamenta in Sveta 2005/29/ES z dne 11. maja 2005 o nepoštenih poslovnih praksah podjetij v razmerju do potrošnikov na notranjem trgu ter o spremembi Direktive Sveta 84/450/EGS, direktiv Evropskega parlamenta in Sveta 97/7/ES, 98/27/ES in 2002/65/ES ter Uredbe (ES) št. 2006/2004 Evropskega parlamenta in Sveta (Direktiva o nepoštenih poslovnih praksah) (UL L 149, 11.6.2005, str. 22).

- (30) Prepovedati bi bilo treba sisteme za biometrično kategorizacijo, ki temeljijo na biometričnih podatkih fizičnih oseb, kot so obraz ali prstni odtisi posameznika, za sklepanje ali ugotavljanje o političnem prepričanju posameznika, članstvu v sindikatu, verskem ali filozofskem prepričanju, rasi, spolnem življenju ali spolni usmerjenosti. Ta prepoved ne bi smela zajemati zakonitega označevanja, filtriranja ali kategorizacije naborov biometričnih podatkov, pridobljenih v skladu s pravom Unije ali nacionalnim pravom na podlagi biometričnih podatkov, kot je razvrščanje slik glede na barvo las ali oči, ki se lahko na primer uporabljajo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.
- (31) Sistemi UI, ki zagotavljajo družbeno točkovanje fizičnih oseb s strani javnih ali zasebnih akterjev, lahko vodijo do diskriminatornih rezultatov in izključitve nekaterih skupin. Lahko kršijo pravico do dostojanstva in nediskriminacije ter vrednote enakosti in pravičnosti. Takšni sistemi UI ocenjujejo ali razvrščajo fizične osebe ali skupine fizičnih oseb na podlagi več podatkovnih točk, povezanih z njihovim družbenim vedenjem v več kontekstih ali znanih, predpostavljenih ali predvidenih osebnih ali osebnostnih značilnostih v določenih časovnih obdobjih. Število družbenih točk, dodeljenih s strani takih sistemov UI, lahko vodi do škodljivega ali neugodnega obravnavanja fizičnih oseb ali celotnih skupin le-teh v družbenih kontekstih, ki niso povezani s kontekstom, v katerem so bili podatki prvotno ustvarjeni ali zbrani, ali do škodljivega obravnavanja, ki je nesorazmerno ali neupravičeno glede na resnost njihovega družbenega vedenja. Sisteme UI, ki vključujejo take nesprejemljive prakse točkovanja in povzročajo takšne škodljive ali neugodne rezultate, bi bilo zato treba prepovedati. Ta prepoved ne bi smela vplivati na zakonite prakse ocenjevanja fizičnih oseb, ki se izvajajo za poseben namen v skladu s pravom Unije in nacionalnim pravom.

- (32) Uporaba sistemov UI za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je posebej hudo poseganje v pravice in svoboščine zadevnih oseb, kolikor lahko vpliva na zasebno življenje velikega dela prebivalstva, vzbuja občutek stalnega nadzora ter posredno odvrča od uresničevanja svobode zbiranja in drugih temeljnih pravic. Tehnične netočnosti sistemov UI, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, lahko vodijo do pristranskih rezultatov in diskriminatornih učinkov. Takšni možni pristranski rezultati in diskriminatorni učinki so zlasti pomembni glede na starost, etnično pripadnost, raso, spol ali invalidnost. Poleg tega se zaradi takojšnjega učinka in omejenih možnosti za nadaljnja preverjanja ali popravke v zvezi z uporabo takih sistemov, ki delujejo v realnem času, povečujejo tveganja za pravice in svoboščine zadevnih oseb v okviru dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali zaradi vpliva teh dejavnosti nanje.

- (33) Zato bi bilo treba prepovedati uporabo teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen v izrecno naštetih in ozko opredeljenih primerih, ko je uporaba nujno potrebna za doseg pomembnega javnega interesa, katerega pomen prevlada nad tveganji. Gre na primer za iskanje nekaterih žrtev kaznivih dejanj, vključno s pogrešanimi osebami, nekatere nevarnosti za življenje ali fizično varnost oseb ali varnost pred terorističnim napadom ter lokalizacijo ali identifikacijo storilcev ali osumljencev kaznivih dejanj, navedenih v prilogi k tej uredbi, kadar je za ta kazniva dejanja v zadevni državi članici predpisana zgornja meja zaporne kazni ali ukrepa, vezanega na odvzem prostosti, najmanj štiri leta in so v pravu te države članice opredeljena. Tak prag za zaporno kazen ali ukrep, vezan na odvzem prostosti, v skladu z nacionalnim pravom prispeva k zagotavljanju, da je kaznivo dejanje dovolj hudo, da bi lahko upravičilo uporabo sistemov za biometrično identifikacijo na daljavo v realnem času. Poleg tega seznam kaznivih dejanj iz priloge k tej uredbi temelji na 32 kaznivih dejanjih, naštetih v Okvirnem sklepu Sveta 2002/584/PNZ¹⁸, ob upoštevanju, da so nekatera od teh kaznivih dejanj v praksi verjetno pomembnejša od drugih, saj bi bila lahko uporaba biometrične identifikacije na daljavo v realnem času predvidoma potrebna in sorazmerna v zelo različnem obsegu za praktično izvajanje lokalizacije ali identifikacije storilca ali osumljenca različnih navedenih kaznivih dejanj ter ob upoštevanju verjetnih razlik v resnosti, verjetnosti in obsegu škode ali morebitnih negativnih posledic.

¹⁸ Okvirni sklep Sveta 2002/584/PNZ z dne 13. junija 2002 o evropskem nalogu za prijetje in postopkih predaje med državami članicami (UL L 190, 18.7.2002, str. 1).

Neposredna grožnja za življenje ali fizično varnost fizičnih oseb bi tudi lahko bila posledica resne motnje v kritični infrastrukturi, kot je opredeljena v členu 2, točka 4, Direktive (EU) 2022/2557 Evropskega parlamenta in Sveta¹⁹, kadar bi okvara ali uničenje take kritične infrastrukture povzročilo neposredno grožnjo za življenje ali fizično varnost osebe, med drugim tako, da bi močno škodilo zagotavljanju osnovne oskrbe prebivalstvu ali izvajanju temeljne funkcije države. Poleg tega bi morala ta uredba organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organom mejne kontrole, organom, pristojnim za priseljevanje, ali azilnim organom še naprej omogočati izvajanje ugotavljanja identitete v prisotnosti zadevne osebe v skladu s pogoji, ki so za tako ugotavljanje določeni v pravu Unije in nacionalnem pravu. Predvsem bi morali imeti organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi mejne kontrole, organi, pristojni za priseljevanje, ali azilni organi možnost, da za identifikacijo oseb, ki med ugotavljanjem identitete tako ugotavljanje zavrnejo ali ne morejo navesti ali dokazati svoje identitete, uporabijo informacijske sisteme v skladu s pravom Unije ali nacionalnim pravom, ne da bi morali v skladu s to uredbo pridobiti predhodno dovoljenje. To bi bila lahko na primer oseba, vpletena v kaznivo dejanje, ki organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ni pripravljena ali zaradi nesreče ali zdravstvenega stanja ne more razkriti svoje identitete.

¹⁹ Direktiva (EU) 2022/2557 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o odpornosti kritičnih subjektov in razveljavitvi Direktive Sveta 2008/114/ES (UL L 333, 27.12.2022, str. 164).

- (34) Za zagotovitev odgovorne in sorazmerne uporabe teh sistemov je pomembno tudi določiti, da bi bilo treba v vsakem od teh izrecno naštetih in ozko opredeljenih primerov upoštevati nekatere elemente, predvsem glede narave razmer, zaradi katerih je bila zahteva vložena, ter posledic uporabe za pravice in svoboščine vseh zadevnih oseb ter zaščitnih ukrepov in pogojev, predvidenih z uporabo. Poleg tega bi bilo treba uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj uporabljati le za potrditev identitete specifično ciljnega posameznika in bi morala biti omejena na to, kar je nujno potrebno za časovno obdobje ter geografsko in osebno področje uporabe, pri čemer je treba upoštevati zlasti dokaze ali znake v zvezi z grožnjami, žrtvami ali storilcem. Uporaba sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih se dovoli le, če je ustrezeni organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj opravil oceno učinka na temeljne pravice in, če v tej uredbi ni določeno drugače, sistem registriral v podatkovni zbirki, kot je določeno v tej uredbi. Referenčna podatkovna zbirka o osebah bi morala biti primerna za vsak primer uporabe v vsakem od navedenih primerov.

- (35) Za vsako uporabo sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj bi bilo treba pridobiti izrecno in posebno dovoljenje sodnega organa ali neodvisnega upravnega organa države članice, katerega odločitev je zavezujoča. Tako dovoljenje bi bilo treba načeloma pridobiti pred uporabo sistema UI za identifikacijo osebe ali oseb. Izjeme od tega pravila bi morale biti dovoljene v ustrezno utemeljenih nujnih primerih iz nujnih razlogov, tj. v primerih, ko je uporaba zadevnih sistemov potrebna do te mere, da je dejansko in objektivno nemogoče pridobiti dovoljenje pred začetkom uporabe sistema UI. V takih nujnih primerih bi bilo treba uporabo sistema UI omejiti na absolutni minimum, zanj pa bi morali veljati ustrezni zaščitni ukrepi in pogoji, kot jih določa nacionalno pravo ter kot jih v okviru vsakega posameznega primera nujne uporabe določi organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Poleg tega bi moral organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v takšnih primerih zaprositi za tako dovoljenje, hkrati pa navesti razloge, zakaj ga ni mogel zahtevati prej, brez nepotrebnega odlašanja in najpozneje v 24 urah. Če se tako dovoljenje zavrne, bi bilo treba takoj prenehati uporabljati sisteme za biometrično identifikacijo v realnem času, povezane s tem dovoljenjem, vse podatke, povezane s tako uporabo, pa bi bilo treba zavreči in izbrisati. Takšni podatki vključujejo vhodne podatke, ki jih sistem UI pridobi neposredno med uporabo takega sistema, ter rezultate in izhodne podatke uporabe, povezane s tem dovoljenjem. Ne bi smeli vključevati vhodnih podatkov, ki so zakonito pridobljeni v skladu z drugim pravom Unije ali nacionalnim pravom. V nobenem primeru odločitve, ki bi imela škodljiv pravni učinek na osebo, ne bi smeli sprejeti izključno na podlagi izhodnih podatkov sistema za biometrično identifikacijo na daljavo.

- (36) Da bi lahko ustrezni organ za nadzor trga in nacionalni organ za varstvo podatkov izvajala svoje naloge v skladu z zahtevami iz te uredbe in nacionalnih pravil, bi ju bilo treba obvestiti o vsaki uporabi sistema za biometrično identifikacijo v realnem času. Organi za nadzor trga in nacionalni organi za varstvo podatkov, ki so bili obveščeni, bi morali Komisiji predložiti letno poročilo o uporabi sistemov za biometrično identifikacijo v realnem času.
- (37) Poleg tega je v izčrpnem okviru, določenem s to uredbo, primerno določiti, da bi morala biti taka uporaba na ozemlju države članice v skladu s to uredbo mogoča le, kadar in kolikor se je zadevna država članica odločila izrecno predvideti možnost odobritve take uporabe v svojih podrobnih pravilih nacionalnega prava. Zato imajo države članice na podlagi te uredbe še naprej pravico, da take možnosti sploh ne predvidijo ali da jo predvidijo le za nekatere cilje, ki lahko upravičijo dovoljeno uporabo, opredeljeno v tej uredbi. O takih nacionalnih predpisih bi bilo treba uradno obvestiti Komisijo v 30 dneh po njihovem sprejetju.

- (38) Uporaba sistemov UI za biometrično identifikacijo fizičnih oseb na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj nujno vključuje obdelavo biometričnih podatkov. Pravila te uredbe, ki ob upoštevanju nekaterih izjem prepovedujejo tako uporabo, ki temelji na členu 16 PDEU, bi se morala uporabljati kot *lex specialis* v zvezi s pravili o obdelavi biometričnih podatkov iz člena 10 Direktive (EU) 2016/680, tako da bi izčrpno urejala tako uporabo in obdelavo zadevnih biometričnih podatkov. Zato bi morali biti taki uporaba in obdelava mogoči le, če sta združljivi z okvirom iz te uredbe, ne da bi zunaj tega okvira obstajalo področje uporabe za pristojne organe, kadar delujejo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za uporabo takih sistemov in obdelavo takih podatkov v zvezi z njimi na podlagi razlogov iz člena 10 Direktive (EU) 2016/680. V tem smislu ta uredba ni namenjena zagotavljanju pravne podlage za obdelavo osebnih podatkov na podlagi člena 8 Direktive (EU) 2016/680. Vendar uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, tudi s strani pristojnih organov, ne bi smela biti zajeta v posebni okvir v zvezi s tako uporabo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, določene s to uredbo. Za tako uporabo za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, zato ne bi smela veljati zahteva po dovoljenju na podlagi te uredbe in veljavnimi podrobnimi pravili nacionalnega prava, na podlagi katerih se lahko to dovoljenje uveljavi.

- (39) Pri vsaki obdelavi biometričnih podatkov in drugih osebnih podatkov, vključenih v uporabo sistemov UI za biometrično identifikacijo, razen v povezavi z uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kot jo ureja ta uredba, bi morale biti še naprej izpolnjene vse zahteve, ki izhajajo iz člena 10 Direktive (EU) 2016/680. Za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, člen 9(1) Uredbe (EU) 2016/679 in člen 10(1) Uredbe (EU) 2018/1725 prepovedujeta obdelavo biometričnih podatkov, za katere veljajo omejene izjeme, kot so določene v navedenih členih. Pri uporabi člena 9(1) Uredbe (EU) 2016/679 za uporabo biometrične identifikacije na daljavo za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, že veljajo odločitve o prepovedi s strani nacionalnih organov za varstvo podatkov.

- (40) V skladu s členom 6a Protokola št. 21 o stališču Združenega kraljestva in Irske v zvezi z območjem svobode, varnosti in pravice, ki je priložen PEU in PDEU, pravila iz člena 5(1), prvi pododstavek, točka (g), kolikor se uporabljajo za uporabo sistemov biometrične kategorizacije za dejavnosti na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah, iz člena 5(1), prvi pododstavek, točka (d), v obsegu, v katerem se uporablja za uporabo sistemov UI, zajetih v navedeni določbi, iz člena 5(1), prvi pododstavek, točka (h), 5(2) do (6) in iz člena 26(10) te uredbe, sprejeta na podlagi člena 16 PDEU, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU, za Irsko niso zavezujoča, če je ne zavezujejo pravila, ki urejajo oblike pravosodnega sodelovanja v kazenskih zadevah ali policijskega sodelovanja, v okviru katerih je treba upoštevati določbe predpisov, sprejetih na podlagi člena 16 PDEU.

- (41) V skladu s členoma 2 in 2a Protokola št. 22 o stališču Danske, ki je priložen PEU in PDEU, Danske ne zavezujejo in se zanje ne uporabljajo pravila iz člena 5(1), prvi pododstavek, točka (g), kolikor se uporabljajo za uporabo sistemov biometrične kategorizacije za dejavnosti na področju policijskega in pravosodnega sodelovanja v kazenskih zadevah, iz člena 5(1), prvi pododstavek, točka (d), v obsegu, v katerem se uporabljata za uporabo sistemov UI, zajetih v navedeni določbi, iz člena 5(1), prvi pododstavek, točka (h), člena 5(2) do (6) in iz člena 26(10) te uredbe, sprejeta na podlagi člena 16 PDEU, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar izvajajo dejavnosti, ki spadajo na področje uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU.

- (42) V skladu z domnevo nedolžnosti bi bilo treba fizične osebe v Uniji zmeraj presoati glede na njihovo dejansko ravnanje. Nikoli jih ne bi smeli presoati na podlagi ravnanja, ki ga predvideva UI zgolj na podlagi njihovega oblikovanja profilov, osebnostnih lastnosti ali značilnosti, kot so državljanstvo, kraj rojstva, kraj prebivališča, število otrok, stopnja zadolženosti ali vrsta avtomobila, brez utemeljenih razlogov za sum, da je bila ta oseba vpletena v kriminalno dejavnost na podlagi objektivnih preverljivih dejstev in brez človeške ocene. Zato bi bilo treba prepovedati ocene tveganja, ki se izvajajo v zvezi s fizičnimi osebami, da se oceni verjetnost, da bodo te osebe storile kaznivo dejanje, ali da se predvidi dejansko ali potencialno kaznivo dejanje samo na podlagi oblikovanja profilov teh fizičnih oseb ali ocene njihovih osebnostnih lastnosti in značilnosti. V nobenem primeru ta prepoved ne vključuje ali se ne nanaša na analizo tveganja, ki ne temelji na oblikovanju profilov oseb ali na osebnostnih lastnostih in značilnostih posameznikov, kot so sistemi UI, ki uporabljajo analizo tveganja za oceno verjetnosti finančnih goljufij s strani podjetij na podlagi sumljivih transakcij ali orodij za analizo tveganja, ki omogočajo napovedovanje verjetnosti lokalizacije prepovedanih drog ali nezakonitega blaga s strani carinskih organov, na primer na podlagi znanih trgovskih poti.
- (43) Treba bi bilo prepovedati dajanje na trg, dajanje v uporabo za ta posebni namen ali uporabo sistemov UI, ki ustvarjajo ali širijo podatkovne zbirke za prepoznavanje obrazov z neciljnim odvzemom podob obraza z interneta ali posnetkov sistema CCTV, saj ta praksa prispeva k občutku množičnega nadzora in lahko povzroči hude kršitve temeljnih pravic, vključno s pravico do zasebnosti.

- (44) Obstajajo resni pomisleki glede znanstvene podlage sistemov UI, katerih namen je prepoznavanje čustev ali sklepanje o njih, zlasti zato, ker se izražanje čustev med kulturami in okoliščinami ter celo pri enem samem posamezniku zelo razlikuje. Med ključnimi pomanjkljivostmi takšnih sistemov so omejena zanesljivost, premajhna specifičnost in omejena možnost posplošitve. Zato lahko sistemi UI, ki prepoznavajo čustva ali namere fizičnih oseb na podlagi svojih biometričnih podatkov ali ki iz njih sklepajo, vodijo do diskriminatornih rezultatov ter posegajo v pravice in svoboščine zadevnih oseb. Glede na neravnovesje moči v kontekstu dela ali izobraževanja ter intruzivne narave teh sistemov bi lahko takšni sistemi povzročili škodljivo ali neugodno obravnavo nekaterih fizičnih oseb ali celotnih skupin fizičnih oseb. Zato bi bilo treba prepovedati dajanje na trg, dajanje v uporabo ali uporabo sistemov UI, namenjenih odkrivanju čustvenega stanja posameznikov v situacijah, povezanih z delovnim mestom in izobraževanjem. Ta prepoved ne bi smela zajemati sistemov UI, danih na trg izključno iz zdravstvenih ali varnostnih razlogov, kot so sistemi za terapevtsko uporabo.
- (45) Ta uredba ne bi smela vplivati na prakse, ki jih prepoveduje pravo Unije, vključno s pravom o varstvu podatkov, pravom o nediskriminaciji, pravom o varstvu potrošnikov in konkurenčnim pravom.

- (46) Visokotvegane sisteme UI bi bilo treba dati na trg Unije ali v uporabo ali jih uporabiti le, če izpolnjujejo nekatere obvezne zahteve. Navedene zahteve bi morale zagotoviti, da visokotvegani sistemi UI, ki so na voljo v Uniji ali katerih izhodni podatki se drugače uporabljajo v Uniji, ne predstavljajo nesprejemljivega tveganja za pomembne javne interese Unije, kot jih priznava in varuje pravo Unije. Kot je pojasnjeno v obvestilu Komisije „Modri vodnik“ o izvajanju pravil EU o proizvodih iz leta 2022²⁰, je na podlagi novega zakonodajnega okvira splošno pravilo, da se več kot en pravni akt harmonizacijske zakonodaje Unije, kot sta uredbi (EU) 2017/745²¹ in (EU) 2017/746²² Evropskega parlamenta in Sveta ter Direktiva 2006/42/ES Evropskega parlamenta in Sveta²³, lahko uporablja za en proizvod, saj se lahko omogočanje dostopnosti ali dajanje v uporabo izvede le, če je proizvod skladen z vso veljavno harmonizacijsko zakonodajo Unije. Da bi zagotovili doslednost in preprečili nepotrebna upravna bremena ali stroške, bi morali ponudnikom proizvoda, ki vsebuje enega ali več visokotveganih sistemov UI, za katere se uporabljajo zahteve iz te uredbe in harmonizacijske zakonodaje Unije iz priloge k tej uredbi, omogočiti prožnost glede operativnih odločitev o tem, kako na optimalen način zagotoviti skladnost proizvoda, ki vsebuje enega ali več sistemov UI, z vsemi veljavnimi zahtevami harmonizacijske zakonodaje Unije. Sistemi UI, opredeljeni kot visokotvegani, bi morali biti omejeni na tiste, ki imajo znaten škodljiv vpliv na zdravje, varnost in temeljne pravice oseb v Uniji, taka omejitev pa bi morala čim bolj zmanjšati morebitno omejevanje mednarodne trgovine.

²⁰ UL C 247, 29.6.2022, str. 1.

²¹ Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1).

²² Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o in vitro diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

²³ Direktiva 2006/42/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o strojih in spremembah Direktive 95/16/ES (UL L 157, 9.6.2006, str. 24).

- (47) Sistemi UI bi lahko imeli škodljiv učinek na zdravje in varnost ljudi, zlasti kadar taki sistemi delujejo kot varnostne komponente proizvodov. V skladu s cilji harmonizacijske zakonodaje Unije, da se olajša prosti pretok proizvodov na notranjem trgu ter zagotovi, da na trg pridejo le varni in skladni proizvodi, je pomembno, da se ustrezno preprečijo in zmanjšajo varnostna tveganja, ki jih lahko povzroči proizvod kot celota zaradi svojih digitalnih komponent, vključno s sistemi UI. Vse bolj avtonomni roboti, ki se uporabljajo v proizvodnji ali za osebno pomoč in oskrbo, bi morali biti na primer sposobni varno delovati in opravljati svoje funkcije v kompleksnih okoljih. Podobno bi morali biti v zdravstvenem sektorju, v katerem je tveganje za življenje in zdravje še posebej veliko, vse bolj izpopolnjeni diagnostični sistemi in sistemi, ki podpirajo človeške odločitve, zanesljivi in točni.

- (48) Pri razvrstitvi sistema UI med sisteme visokega tveganja je zlasti pomemben obseg škodljivega vpliva sistema UI na temeljne pravice, varovane z Listino. Te pravice vključujejo pravico do človekovega dostojanstva, spoštovanja zasebnega in družinskega življenja, varstvo osebnih podatkov, svobodo izražanja in obveščanja, svobodo zbiranja in združevanja, pravico do nediskriminacije, pravico do izobraževanja, varstvo potrošnikov, pravice delavcev, pravice invalidov, enakost spolov, pravice intelektualne lastnine, pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, pravico do obrambe in domneve nedolžnosti ter pravico do dobrega upravljanja. Poleg teh pravic je treba poudariti tudi dejstvo, da imajo otroci posebne pravice, zapisane v členu 24 Listine in v Konvenciji Združenih narodov o otrokovih pravicah (v zvezi z digitalnim okoljem ter podrobneje opredeljene v splošni pripombi št. 25 KZNOP), ki zahtevata upoštevanje šibkih točk otrok ter zagotavljanje zaščite in varstva, ki sta potrebna za njihovo dobro počutje. Pri ocenjevanju resnosti škode, ki jo lahko povzroči sistem UI, je treba upoštevati tudi temeljno pravico do visoke ravni varstva okolja, ki je zapisana v Listini in se izvaja v politikah Unije, tudi v zvezi z zdravjem in varnostjo oseb.

- (49) Kar zadeva visokotvegane sisteme UI, ki so varnostne komponente proizvodov ali sistemov ali so sami proizvodi ali sistemi, ki spadajo na področje uporabe Uredbe (ES) št. 300/2008 Evropskega parlamenta in Sveta²⁴, Uredbe (EU) št. 167/2013 Evropskega parlamenta in Sveta²⁵, Uredbe (EU) št. 168/2013 Evropskega parlamenta in Sveta²⁶, Direktive 2014/90/EU Evropskega parlamenta in Sveta²⁷, Direktive (EU) 2016/797 Evropskega parlamenta in Sveta²⁸,

²⁴ Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (UL L 97, 9.4.2008, str. 72);

²⁵ Uredba (EU) št. 167/2013 Evropskega parlamenta in Sveta z dne 5. februarja 2013 o odobritvi in tržnem nadzoru kmetijskih in gozdarskih vozil (UL L 60, 2.3.2013, str. 1).

²⁶ Uredba (EU) št. 168/2013 Evropskega parlamenta in Sveta z dne 15. januarja 2013 o odobritvi in tržnem nadzoru dvo- ali trikolesnih vozil in štirikolesnikov (UL L 60, 2.3.2013, str. 52).

²⁷ Direktiva 2014/90/EU Evropskega parlamenta in Sveta z dne 23. julija 2014 o pomorski opremi in razveljavitvi Direktive Sveta 96/98/ES (UL L 257, 28.8.2014, str. 146).

²⁸ Direktiva (EU) 2016/797 Evropskega parlamenta in Sveta z dne 11. maja 2016 o interoperabilnosti železniškega sistema v Evropski uniji (UL L 138, 26.5.2016, str. 44).

Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta²⁹, Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta³⁰ ter Uredbe (EU) 2019/2144 Evropskega parlamenta in Sveta³¹, je primerno spremeniti navedene akte, da bi zagotovili, da Komisija na podlagi tehničnih in regulativnih posebnosti vsakega sektorja ter brez poseganja v obstoječe mehanizme upravljanja, ugotavljanja skladnosti in izvrševanja ter delo organov, določenih v njih, pri sprejemanju ustreznih delegiranih ali izvedbenih aktov v skladu z navedenimi akti upošteva obvezne zahteve za visokotvegane sisteme UI iz te uredbe.

²⁹ Uredba (EU) 2018/858 Evropskega parlamenta in Sveta z dne 30. maja 2018 o odobritvi in tržnem nadzoru motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, spremembi uredb (ES) št. 715/2007 in (ES) št. 595/2009 ter razveljavitvi Direktive 2007/46/ES (UL L 151, 14.6.2018, str. 1).

³⁰ Uredba (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 (UL L 212, 22.8.2018, str. 1).

³¹ Uredba (EU) 2019/2144 Evropskega parlamenta in Sveta z dne 27. novembra 2019 o zahtevah za homologacijo motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, v zvezi z njihovo splošno varnostjo in zaščito potnikov v vozilu ter izpostavljenih udeležencev v cestnem prometu in o spremembi Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 78/2009, (ES) št. 79/2009 in (ES) št. 661/2009 Evropskega parlamenta in Sveta in uredb Komisije (ES) št. 631/2009, (EU) št. 406/2010, (EU) št. 672/2010, (EU) št. 1003/2010, (EU) št. 1005/2010, (EU) št. 1008/2010, (EU) št. 1009/2010, (EU) št. 19/2011, (EU) št. 109/2011, (EU) št. 458/2011, (EU) št. 65/2012, (EU) št. 130/2012, (EU) št. 347/2012, (EU) št. 351/2012, (EU) št. 1230/2012 in (EU) 2015/166 (UL L 325, 16.12.2019, str. 1).

- (50) Kar zadeva sisteme UI, ki so varnostne komponente proizvodov ali so sami proizvodi s področja uporabe določene harmonizacijske zakonodaje Unije, navedene v prilogi k tej uredbi, jih je primerno na podlagi te uredbe razvrstiti med sisteme visokega tveganja, če je zadevni proizvod v postopku ugotavljanja skladnosti pri organu, ki izvaja ugotavljanje skladnosti s strani tretjih oseb na podlagi ustrezne harmonizacijske zakonodaje Unije. Taki proizvodi so zlasti stroji, igrače, dvigala, oprema in zaščitni sistemi za uporabo v potencialno eksplozivnih atmosferah, radijska oprema, tlačna oprema, oprema za plovila za rekreacijo, žičniške naprave, naprave, v katerih zgoreva plinasto gorivo, medicinski pripomočki in vitro diagnostični medicinski pripomočki, avtomobili in letala.
- (51) Razvrstitev sistema UI kot visokotveganega na podlagi te uredbe ne bi smela nujno pomeniti, da se proizvod, katerega varnostna komponenta je sistem UI, ali sam sistem UI kot proizvod šteje za visokotvegan na podlagi meril iz ustrezne harmonizacijske zakonodaje Unije, ki se uporablja za proizvod. To zlasti velja za uredbi (EU) 2017/745 in (EU) 2017/746, pri katerih je ugotavljanje skladnosti, ki ga opravi tretja oseba, zagotovljeno za izdelke srednjega in visokega tveganja.

- (52) Kar zadeva samostojne sisteme UI in zlasti visokotvegane sisteme UI, razen tistih, ki so varnostne komponente proizvodov ali ki so sami proizvodi, jih je primerno razvrstiti kot sisteme visokega tveganja, če glede na svoj predvideni namen predstavljajo visoko tveganje škode za zdravje in varnost ali temeljne pravice oseb, ob upoštevanju resnosti možne škode in verjetnosti njenega nastanka, ter se uporabljajo na več posebej vnaprej opredeljenih področjih, določenih v Uredbi. Opredelitev teh sistemov temelji na isti metodologiji in merilih, kot so predvideni tudi za morebitne prihodnje spremembe seznama visokotveganih sistemov UI, za katere bi bilo treba Komisijo pooblastiti, da jih sprejme z delegiranimi akti, da bi upoštevali hiter tehnološki razvoj in morebitne spremembe v uporabi sistemov UI.

- (53) Treba je tudi pojasniti, da lahko obstajajo posebni primeri, v katerih sistemi UI, ki se nanašajo na vnaprej določena področja, navedena v tej uredbi, ne povzročajo znatnega tveganja škode za pravne interese, zaščitene na teh področjih, ker ne vplivajo bistveno na odločanje ali ne škodujejo bistveno tem interesom. Za namene te uredbe bi bilo treba sistem UI, ki ne vpliva bistveno na izid odločanja, razumeti kot sistem UI, ki ne vpliva na vsebino in s tem na rezultat odločanja, bodisi človeškega ali avtomatiziranega. Sistem UI, ki ne vpliva bistveno na izid odločanja, bi lahko vključeval primere, v katerih je izpolnjen eden ali več naslednjih pogojev. Prvi tak pogoj bi moral biti, da je sistem UI namenjen opravljanju ozke postopkovne naloge, kot je sistem UI, ki nestrukturirane podatke pretvori v strukturirane podatke, sistem UI, ki prejete dokumente razvršča v kategorije, ali sistem UI, ki se uporablja za odkrivanje duplikatov v številnih aplikacijah. Te naloge so tako ozke in omejene, da predstavljajo le omejena tveganja, ki se z uporabo sistema UI v okviru, ki je v prilogi k tej uredbi naveden kot uporaba, povezana z visokim tveganjem, ne povečajo. Drugi pogoj bi moral biti, da je namen naloge, ki jo opravlja sistem UI, izboljšati rezultat predhodno zaključene človeške dejavnosti, ki bi lahko bila pomembna za namene visokotvegane uporabe, navedene v prilogi k tej uredbi. Glede na te značilnosti sistem UI zagotavlja le dodatno plast človeške dejavnosti s posledično manjšim tveganjem. Ta pogoj bi se na primer uporabljal za sisteme UI, katerih namen je izboljšati jezik, ki se uporablja v predhodno pripravljenih dokumentih, na primer v zvezi s poklicnim tonom, akademskim slogom jezika ali uskladitvijo besedila s sporočili določene blagovne znamke. Tretji pogoj bi moral biti, da je sistem UI namenjen odkrivanju vzorcev odločanja ali odstopanj od vzorcev predhodnega odločanja.

Tveganje bi se zmanjšalo, ker uporaba sistema UI sledi predhodno opravljeni človeški oceni in ni namenjena temu, da bi jo nadomestila ali nanjo vplivala brez ustreznega človeškega pregleda. Takšni sistemi UI vključujejo na primer sisteme, ki se lahko glede na določen vzorec, po katerem neki učitelj ocenjuje, uporabijo za naknadno preverjanje, ali je učitelj morda odstopal od tega vzorca, da bi opozorili na morebitne nedoslednosti ali nepravilnosti. Četrty pogoj bi moral biti, da je sistem UI namenjen opravljanju naloge, ki je le pripravljalna za oceno, relevantno za namene sistemov UI, navedenih v prilogi k tej uredbi, s čimer bi bil morebitni učinek izhodnih podatkov sistema zelo majhen v smislu tveganja, ki ga je treba upoštevati pri oceni. Ta pogoj med drugim zajema pametne rešitve za ravnanje z datotekami, ki vključujejo različne funkcije, kot so indeksiranje, iskanje, obdelava besedil in govora ali povezovanje podatkov z drugimi viri podatkov, ali sisteme UI, ki se uporabljajo za prevajanje prvotnih dokumentov. V vsakem primeru bi bilo treba šteti, da sistemi UI, ki se uporabljajo v primerih uporabe visokega tveganja, navedeni v prilogi k tej uredbi, predstavljajo znatno tveganje škode za zdravje, varnost ali temeljne pravice, če sistem UI vključuje oblikovanje profilov v smislu člena 4, točka 4, Uredbe (EU) 2016/679 ali člena 3, točka 4, Direktive (EU) 2016/680 ali člena 3, točka 5, Uredbe (EU) 2018/1725. Da bi zagotovili sledljivosti in preglednost, bi moral ponudnik, ki meni, da sistem UI na podlagi zgoraj navedenih pogojev ne predstavlja visokega tveganja, pripraviti dokumentacijo o oceni, preden se ta sistem da na trg ali v uporabo, in bi moral to dokumentacijo na zahtevo predložiti pristojnim nacionalnim organom. Takšen ponudnik bi moral sistem UI registrirati v podatkovni zbirki EU, vzpostavljeni s to uredbo. Da bi zagotovili dodatne smernice za praktično izvajanje pogojev, pod katerimi sistemi UI navedeni v prilogi k tej uredbi, izjemoma ne predstavljajo visokega tveganja, bi morala Komisija po posvetovanju z Odborom zagotoviti smernice, v katerih bi bilo določeno, da se praktično izvajanje dopolni s celovitim seznamom praktičnih primerov uporabe visoko tveganih sistemov UI in sistemov UI, ki to niso.

- (54) Ker so biometrični podatki posebna kategorija osebnih podatkov, je primerno, da se več kritičnih primerov uporabe biometričnih sistemov razvrsti kot visokotvegane, če je njihova uporaba dovoljena na podlagi ustreznega prava Unije in nacionalnega prava. Tehnične netočnosti sistemov UI, namenjenih za biometrično identifikacijo fizičnih oseb na daljavo, lahko vodijo do pristranskih rezultatov in diskriminatornih učinkov. Tveganje takšnih pristranskih rezultatov in diskriminatornih učinkov je zlasti pomembno v zvezi s starostjo, etnično pripadnostjo, raso, spolom ali invalidnostjo. Glede na tveganja, ki jih predstavljajo sistemi za biometrično identifikacijo na daljavo, bi jih bilo treba razvrstiti kot sisteme visokega tveganja. Takšna razvrstitev izključuje sisteme UI za biometrično preverjanje, tudi avtentikacijo, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja, in potrditi identiteto fizične osebe izključno zaradi dostopa do storitve, odklepanja naprave ali varnega dostopa do prostorov. Poleg tega bi bilo kot sisteme visokega tveganja treba razvrstiti sisteme UI, namenjene uporabi za biometrično kategorizacijo v skladu z občutljivimi lastnostmi ali značilnostmi, zaščitenimi na podlagi člena 9(1) Uredbe (EU) 2016/679 na podlagi biometričnih podatkov, če ti niso prepovedani s to uredbo, in sisteme za prepoznavanje čustev, ki niso prepovedani s to uredbo. Biometrični sistemi, ki naj bi se uporabljali izključno za omogočanje ukrepov za kibernetko varnost in varstvo osebnih podatkov, ne bi smeli šteti za visokotvegane sisteme UI.

- (55) V zvezi z upravljanjem in delovanjem kritične infrastrukture je primerno, da se sistemi UI, namenjeni uporabi kot varnostne komponente pri upravljanju in delovanju kritične digitalne infrastrukture, navedene v točki 8 iz Priloge k Direktivi (EU) 2022/2557, cestnega prometa ter oskrbi z vodo, plinom, ogrevanjem in električno energijo, razvrstijo kot sistemi visokega tveganja, saj lahko njihovo nedelovanje ali okvara delovanja ogrožajo življenje in zdravje ljudi v velikem obsegu ter povzročijo občutne motnje v rednem izvajanju družbenih in gospodarskih dejavnosti. Varnostne komponente kritične infrastrukture, vključno s kritično digitalno infrastrukturo, so sistemi, ki se uporabljajo za neposredno zaščito fizične celovitosti kritične infrastrukture ali zdravja in varnosti oseb in premoženja, vendar niso potrebne za delovanje sistema. Nedelovanje ali okvara takih komponent bi lahko povzročila neposredno tveganje za fizično celovitost kritične infrastrukture ter posledično tveganje za zdravje in varnost oseb in premoženja. Komponente, namenjene izključno za uporabo v namene kibernetске varnosti, ne bi smele škodovati za varnostne komponente. Primeri varnostnih komponent takšne kritične infrastrukture lahko vključujejo sisteme za spremljanje vodnega tlaka ali sisteme za upravljanje požarnega alarma v okviru centrov računalništva v oblaku.

- (56) Uvajanje sistemov UI v izobraževanju je pomembno za spodbujanje visokokakovostnega digitalnega izobraževanja in usposabljanja, da bi vsem učencem in učiteljem omogočili pridobivanje in deljenje potrebnih digitalnih spretnosti in kompetenc, vključno z medijsko pismenostjo in kritičnim razmišljanjem ter s tem dejavno sodelovanje v gospodarstvu, družbi in demokratičnih procesih. Vendar bi bilo treba sisteme UI, ki se uporabljajo v izobraževanju ali poklicnem usposabljanju, zlasti za določanje dostopa ali sprejema ali za razvrščanje fizičnih oseb v izobraževalne ustanove ali programe in ustanove ali programe za poklicno usposabljanje na vseh ravneh za ocenjevanje učnih izidov oseb, ustrezne ravni izobrazbe posameznika in materialno vplivanje na raven izobraževanja in usposabljanja, ki jo bodo posamezniki prejeli ali bodo lahko dostopali do nje ali za spremljanje in odkrivanje prepovedanega vedenja študentov med testi, razvrstiti kot visokotvegane sisteme UI, saj lahko določajo izobraževalni in poklicni potek življenja osebe in lahko zato vplivajo na zmožnost te osebe, da si zagotovi preživetje. Če so takšni sistemi neustrezno zasnovani in uporabljeni, lahko zlasti hudo posegajo v pravico do izobraževanja in usposabljanja ter pravico do nediskriminacije in ju lahko kršijo ter ohranjajo vzorce diskriminacije iz preteklosti, na primer žensk, nekaterih starostnih skupin, invalidov ali oseb določenega rasnega ali etničnega porekla ali spolne usmerjenosti.

- (57) Sisteme UI, ki se uporabljajo pri zaposlovanju, upravljanju delavcev in dostopu do samozaposlitve, zlasti za zaposlovanje in izbor oseb, za sprejemanje odločitev, ki vplivajo na delovne pogoje, napredovanje ali prenehanje pogodbenih delovnih razmerij, za dodeljevanje nalog na podlagi individualnega vedenja, osebnih lastnosti ali značilnosti ter za spremljanje ali ocenjevanje oseb v z delom povezanih pogodbenih razmerjih, bi bilo treba prav tako razvrstiti med sisteme visokega tveganja, saj lahko ti sistemi občutno vplivajo na prihodnje poklicne možnosti, možnosti preživljanja teh oseb in pravice delavcev. Ustrezna pogodbeno delovna razmerja bi morala smiselno vključevati zaposlene in osebe, ki zagotavljajo storitve preko platform, ki so navedene v delovnem programu Komisije za leto 2021. V celotnem postopku zaposlovanja in pri ocenjevanju, napredovanju ali ohranjanju oseb v pogodbenih delovnih razmerjih lahko taki sistemi ohranjajo vzorce diskriminacije iz preteklosti, na primer nad ženskami, določenimi starostnimi skupinami, invalidi ali osebami določenega rasnega ali etničnega porekla ali spolne usmerjenosti. Tudi sistemi UI, ki se uporabljajo za spremljanje učinkovitost in vedenja teh oseb, lahko ogrožajo njihove temeljne pravice do varstva podatkov in zasebnosti.

- (58) Drugo področje, na katerem je treba posebno pozornost nameniti uporabi sistemov UI, je dostop do nekaterih bistvenih zasebnih in javnih storitev ter koristi, ki jih ljudje potrebujejo za polno udeležbo v družbi ali izboljšanje življenjskega standarda. Zlasti fizične osebe, ki zaprosijo za ali od javnih organov prejemajo bistvene ugodnosti in storitve javne pomoči, in sicer zdravstvene storitve, dajatve socialne varnosti, socialne storitve, ki zagotavljajo zaščito v primerih, kot so materinstvo, bolezen, nesreče pri delu, odvisnost ali starost ter izguba zaposlitve ter socialna in stanovanjska pomoč, so običajno odvisne od teh ugodnosti in storitev ter so v ranljivem položaju v odnosu do odgovornih organov. Če se sistemi UI uporabljajo za določanje, ali naj organi take ugodnosti in storitveodobrijo, zavrnejo, zmanjšajo, prekličejo ali zahtevajo povračilo, vključno s tem, ali so upravičenci legitimno upravičeni do takih ugodnosti ali storitev, lahko ti sistemi pomembno vplivajo na preživljanje oseb in kršijo njihove temeljne pravice, kot so pravica do socialne zaščite, nediskriminacije, človekovega dostojanstva ali učinkovitega pravnega sredstva, in bi zato morali biti opredeljeni kot visokotvegani sistemi UI. Kljub temu ta uredba ne bi smela ovirati razvoja in uporabe inovativnih pristopov v javni upravi, ki bi imela koristi od širše uporabe skladnih in varnih sistemov UI, če ti sistemi ne pomenijo visokega tveganja za pravne in fizične osebe.

Poleg tega bi bilo treba sisteme UI, ki se uporabljajo za ocenjevanje kreditne ocene ali kreditne sposobnosti fizičnih oseb, razvrstiti kot visokotvegane sisteme UI, saj določajo dostop teh oseb do finančnih sredstev ali bistvenih storitev, kot so stanovanja, električna energija in telekomunikacijske storitve. Sistemi UI, ki se uporabljajo v te namene, lahko povzročijo diskriminacijo oseb ali skupin in ohranijo vzorce diskriminacije iz preteklosti, na primer na podlagi rasnega ali etničnega porekla, spola, invalidnosti, starosti ali spolne usmerjenosti, ali ustvarijo nove oblike diskriminatornih vplivov. Vendar sistemi UI, ki so v pravu Unije določeni za namene odkrivanja goljufij pri ponujanju finančnih storitev ter za bonitetne namene za izračun kapitalskih zahtev kreditnih institucij in zavarovalnic, na podlagi te uredbe ne bi smeli škodovati za sisteme visokega tveganja. Poleg tega lahko sistemi UI, namenjeni za oceno tveganja in oblikovanje cen v zvezi s fizičnimi osebami za zdravstveno in življenjsko zavarovanje, tudi pomembno vplivajo na preživetje oseb in lahko, če niso ustrezno zasnovani, razviti in uporabljeni, kršijo njihove temeljne pravice in povzročijo resne posledice za življenje in zdravje ljudi, vključno s finančno izključenostjo in diskriminacijo. Poleg tega bi bilo treba sisteme UI, ki se uporabljajo za ocenjevanje in razvrščanje klicev v sili fizičnih oseb ali za pošiljanje ali določanje prednosti pri napotitvi služb za ukrepanje ob nesrečah, vključno s policijo, gasilci in medicinsko pomočjo, ter sistemih triaže pacientov v nujnem zdravstvenem varstvu, razvrstiti med sisteme visokega tveganja, saj sprejemajo odločitve v zelo kritičnih razmerah za življenje in zdravje oseb ter njihovo premoženje.

- (59) Glede na vlogo in odgovornost organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, je za njihove ukrepe, ki vključujejo nekatere uporabe sistemov UI, značilna precejšnja stopnja neravnovesja moči, kar lahko vodi do nadzora, prijetja ali odvzema prostosti fizične osebe ter drugih škodljivih vplivov na temeljne pravice, ki jih zagotavlja Listina. Zlasti če se sistem UI ne uči z visokokakovostnimi podatki, ne izpolnjuje ustreznih zahtev glede zmogljivosti, točnosti ali robustnosti ali ni ustrezno zasnovan in testiran, preden je dan na trg ali na kakšen drug način v uporabo, lahko ljudi izpostavi na diskriminatoren ali kako drugače napačen ali nepravičen način. Poleg tega bi lahko bilo ovirano uveljavljanje pomembnih procesnih temeljnih pravic, kot so pravica do učinkovitega pravnega sredstva in nepristranskega sodišča ter pravica do obrambe in domneve nedolžnosti, zlasti kadar taki sistemi UI niso dovolj pregledni, obrazložljivi in dokumentirani. Zato je primerno, da se številni sistemi UI, kolikor je njihova uporaba dovoljena na podlagi zadevnega prava Unije in nacionalnega prava, namenjeni uporabi v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razvrstijo med sisteme visokega tveganja, kjer so točnost, zanesljivost in preglednost še posebej pomembni, da se preprečijo škodljivi vplivi, ohrani zaupanje javnosti ter zagotovita odgovornost in učinkovito sodno varstvo.

Glede na naravo dejavnosti in s tem povezana tveganja bi morali ti visokotvegani sistemi UI vključevati zlasti sisteme UI, ki so namenjeni uporabi s strani ali v imenu organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali institucij, organov, uradov ali agencij Unije v podporo tem organom pri ocenjevanju tveganja, da fizična oseba postane žrtev kaznivih dejanj, kot so poligrafi in podobna orodja, za ocenjevanje zanesljivosti dokazov med preiskovanjem ali pregonom kaznivih dejanj in, če to ni prepovedano na podlagi te uredbe, za ocenjevanje tveganja, da fizična oseba stori ali ponovi kaznivo dejanje, ne izključno na podlagi oblikovanja profilov fizičnih oseb ali ocene osebnostnih lastnosti in značilnosti ali preteklega kaznivega ravnanja fizičnih oseb ali skupin, za oblikovanje profilov med odkrivanjem, preiskovanjem ali pregonom kaznivih dejanj. Sistemi UI, posebej namenjeni uporabi v upravnih postopkih s strani davčnih in carinskih organov ter finančnoobveščevalnih enot, ki izvajajo upravne naloge analiziranja informacij na podlagi prava Unije o preprečevanju pranja denarja, ne bi smeli biti opredeljeni kot visokotvegani sistemi UI, ki jih uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za namen preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj. Organi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in drugi ustrezni organi orodij UI ne bi smeli uporabljati tako, da bi postala dejavnik pri neenakosti ali izključenosti. Ne bi smeli zanemariti vpliva uporabe orodij UI na pravice osumljencev do obrambe, zlasti težav pri pridobivanju smiselnih informacij o delovanju teh sistemov in posledičnih težav pri izpodbijanju njihovih rezultatov na sodišču, zlasti s strani fizičnih oseb, ki so predmet preiskave.

- (60) Sistemi UI, ki se uporabljajo pri upravljanju migracij, azila in nadzora meje, vplivajo na osebe, ki so pogosto v posebej ranljivem položaju ter so odvisne od izida ukrepov pristojnih javnih organov. Točnost, nediskriminatornost in preglednost sistemov UI, ki se uporabljajo v teh kontekstih, so zato zlasti pomembni za zagotavljanje spoštovanja temeljnih pravic zadevnih oseb, zlasti njihovih pravic do prostega gibanja, nediskriminacije, varstva zasebnega življenja in osebnih podatkov, mednarodnega varstva in dobrega upravljanja. Zato je primerno, da se med sisteme visokega tveganja razvrstijo sistemi UI, ki so na podlagi ustreznega prava Unije in nacionalnega prava dovoljeni za uporabo s strani ali v imenu pristojnih javnih organov ali institucij, organov, uradov ali agencij Unije, zadolženih za naloge na področju migracij, azila in upravljanja nadzora meja, kot so poligrafi in podobna orodja, za ocenjevanje nekaterih tveganj, ki jih predstavljajo fizične osebe, ki vstopajo na ozemlje države članice ali zaprosijo za vizum ali azil, za pomoč pristojnim javnim organom pri obravnavi, vključno s povezano oceno zanesljivosti dokazov, prošenj za azil, vizumov in dovoljenj za prebivanje ter s tem povezanih pritožb zaradi ugotavljanja upravičenosti fizičnih oseb, ki zaprosijo za status, za namene odkrivanja, priznavanja ali identifikacije fizičnih oseb v okviru upravljanja migracij, azila in nadzora meje, z izjemo preverjanja potnih listin.

Sistemi UI na področju migracij, azila in upravljanja nadzora meja, ki jih zajema ta uredba, bi morali biti skladni z ustreznimi postopkovnimi zahtevami iz Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta³², Direktive 2013/32/EU Evropskega parlamenta in Sveta³³ ter drugega ustreznega prava Unije. Države članice ali institucije, organi, uradi ali agencije Unije v nobenem primeru ne bi smeli uporabljati sistemov UI na področju migracij, azila in upravljanja nadzora meja kot sredstvo za izogibanje svojim mednarodnim obveznostim iz Konvencije ZN o statusu beguncev, podpisane v Ženevi 28. julija 1951, kakor je bila spremenjena s Protokolom z dne 31. januarja 1967. Prav tako se ne smejo uporabljati za kakršno koli kršitev načela nevračanja ali za odrekanje varnih in učinkovitih zakonitih poti na ozemlje Unije, vključno s pravico do mednarodne zaščite.

³² Uredba (ES) št. 810/2009 Evropskega parlamenta in Sveta z dne 13. julija 2009 o vizumskem zakoniku Skupnosti (Vizumski zakonik) (UL L 243, 15.9.2009, str. 1).

³³ Direktiva 2013/32/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o skupnih postopkih za priznanje ali odvzem mednarodne zaščite (UL L 180, 29.6.2013, str. 60).

- (61) Nekatere sisteme UI, namenjene razsojanju in demokratičnim procesom, bi bilo treba razvrstiti med sisteme visokega tveganja zaradi njihovega potencialno pomembnega vpliva na demokracijo, pravno državo, osebne svoboščine ter pravico do učinkovitega pravnega sredstva in nepristranskega sodišča. Zlasti zato, da bi zmanjšali tveganja morebitnih pristranskosti, napak in nepreglednosti, je primerno, da se visokotvegani sistemi UI, namenjeni uporabi s strani sodnega organa ali v njegovem imenu za pomoč sodnim organom pri raziskovanju in razlagi dejstev in prava ter pri uporabi prava za konkreten sklop dejstev, opredelijo kot sistemi visokega tveganja. Tudi sisteme UI, ki naj bi jih za te namene uporabljali organi za alternativno reševanje sporov, bi bilo treba šteti za sisteme visokega tveganja, če imajo rezultati postopkov alternativnega reševanja sporov pravne učinke za stranke. Orodja UI se lahko uporabljajo kot pomoč sodnikom pri odločanju ali podpora neodvisnosti sodstva, vendar jih ne bi smela nadomeščati: končno odločanje mora ostati dejavnost, ki jo vodi človek. Razvrščanje sistemov UI kot sistemov visokega tveganja pa se ne bi smelo uporabljati tudi za sisteme UI, namenjene izključno pomožnim upravnim dejavnostim, ki ne vplivajo na dejansko razsojanje v posameznih primerih, kot so anonimizacija ali psevdonimizacija sodnih odločb, dokumentov ali podatkov, komunikacije med osebjem ali upravnih nalog.

- (62) Brez poseganja v pravila iz Uredbe (EU) 2024/... Evropskega parlamenta in Sveta³⁴⁺ ter za obravnavanje tveganj neupravičenega zunanjega poseganja v volilno pravico iz člena 39 Listine in nesorazmernih učinkov na demokracijo in pravno državo bi bilo treba sisteme UI, namenjene vplivanju na izid volitev ali referendumov ali na volilno vedenje fizičnih oseb pri glasovanju na volitvah ali referendumih, razvrstiti kot visokotvegane sisteme UI, razen kadar gre za sisteme UI, pri katerih fizične osebe niso neposredno izpostavljene njihovim izhodnim podatkom, kot so orodja, ki se uporabljajo za organizacijo, optimizacijo in strukturiranje političnih kampanj z upravnega in logističnega vidika.
- (63) Dejstva, da je sistem UI na podlagi te uredbe razvrščen kot visokotvegani sistem UI, se ne bi smelo razlagati tako, da pomeni, da je njegova uporaba zakonita na podlagi drugih aktov prava Unije ali na podlagi nacionalnega prava, združljivim s pravom Unije, kot so varstvo osebnih podatkov, uporaba poligrafov in podobnih orodij ali drugih sistemov za zaznavanje čustvenega stanja fizičnih oseb. Vsaka taka uporaba bi se morala še naprej izvajati izključno v skladu z veljavnimi zahtevami, ki izhajajo iz Listine ter veljavnih aktov sekundarnega prava Unije in nacionalnega prava. Te uredbe ne bi smeli razumeti kot pravne podlage za obdelavo osebnih podatkov, vključno s posebnimi vrstami osebnih podatkov, kadar je to ustrezno, razen če je v tej uredbi izrecno določeno drugače.

³⁴ Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o preglednosti in ciljanem političnem oglaševanju (UL L, ..., ELI: ...).

⁺ UL: prosimo, da v besedilo vstavite številko uredbe iz dokumenta PE 90/23 (2021/0381(COD)) in dopolnite pripadajočo opombo.

- (64) Da bi zmanjšali tveganja iz visokotveganih sistemov UI, ki so dani na trg ali v uporabo, in zagotovili visoko raven zanesljivosti, bi bilo treba za visokotvegane sisteme UI uporabljati nekatere obvezne zahteve in pri tem upoštevati predvideni namen in kontekst uporabe sistema UI ter sistem obvladovanja tveganja, ki ga vzpostavi ponudnik. Ponudniki bi pri ukrepih, ki jih sprejmejo za izpolnjevanje obveznih zahtev iz te uredbe, morali upoštevati splošno priznane najsodobnejše tehnološke dosežke na področju UI; ti ukrepi bi morali biti sorazmerni in učinkoviti za doseganje ciljev te uredbe. Kot je pojasnjeno v obvestilu Komisije „Modri vodnik“ o izvajanju pravil EU o proizvodih iz leta 2022, je na podlagi novega zakonodajnega okvira splošno pravilo, da se več kot en pravni akt harmonizacijske zakonodaje Unije lahko uporablja za en proizvod, saj se lahko dostopnost ali dajanje v uporabo izvede le, če je proizvod skladen z vso veljavno harmonizacijsko zakonodajo Unije. Nevarnosti sistemov UI, za katere veljajo zahteve iz te uredbe, se nanašajo na vidike, ki se razlikujejo od obstoječe harmonizacijske zakonodaje Unije, zato naj bi zahteve iz te uredbe dopolnjevale obstoječi del harmonizacijske zakonodaje Unije. Na primer stroji ali medicinski pripomočki, ki vključujejo sistem UI, lahko pomenijo tveganja, ki v bistvenih zdravstvenih in varnostnih zahtevah iz ustrezne harmonizirane zakonodaje Unije niso zajeta, saj navedeno sektorsko pravo ne obravnava tveganj, značilnih za sisteme UI.

To zahteva hkratno in dopolnjevalno uporabo različnih zakonodajnih aktov. Da bi zagotovili doslednost in preprečili nepotrebno upravno breme ali nepotrebne stroške, bi morali ponudnikom proizvoda, ki vsebuje enega ali več visokotveganih sistemov UI, za katere se uporabljajo zahteve iz te uredbe in harmonizacijske zakonodaje Unije, ki temelji na novem zakonodajnem okviru in je navedena v prilogi k tej uredbi, omogočiti prožnost glede operativnih odločitev o tem, kako na optimalen način zagotoviti skladnost proizvoda, ki vsebuje enega ali več sistemov UI, z vsemi veljavnimi zahtevami harmonizirane zakonodaje Unije. Ta prožnost bi lahko na primer pomenila odločitev ponudnika, da del potrebnih postopkov testiranja in poročanja, informacij in dokumentacije, ki se zahtevajo na podlagi te uredbe, vključi v dokumentacijo in postopke, ki že obstajajo in se zahtevajo na podlagi harmonizacijske zakonodaje Unije, ki temelji na novem zakonodajnem okviru in je navedena v prilogi k tej uredbi. To nikakor ne bi smelo ogroziti obveznosti ponudnika, da izpolnjuje vse veljavne zahteve.

- (65) Sestavni del sistema obvladovanja tveganja bi moral biti neprekinjen ponavljajoč se proces, ki se načrtuje in izvaja v celotnem življenjskem ciklu visokotveganega sistema UI. Ta proces bi moral biti usmerjen v prepoznavanje in zmanjšanje relevantnih tveganj sistemov UI za zdravje, varnost in temeljne pravice. Sistem obvladovanja tveganj bi bilo treba redno pregledovati in posodablјati, da bi zagotovili njegovo stalno učinkovitost ter utemeljitev in dokumentiranje vseh pomembnih odločitev in ukrepov, sprejetih v skladu s to uredbo. S tem postopkom bi bilo treba zagotoviti, da ponudnik opredeli tveganja ali škodljive vplive ter izvaja ukrepe za zmanjšanje znanih in razumno predvidljivih tveganj sistemov UI za zdravje, varnost in temeljne pravice glede na njihov predvideni namen in razumno predvidljivo napačno uporabo, vključno z morebitnimi tveganji, ki izhajajo iz interakcije med sistemom UI in okoljem, v katerem deluje. V okviru sistema obvladovanja tveganj bi bilo treba sprejeti najprimernejše ukrepe za obvladovanje tveganja glede na najsodobnejše tehnološke dosežke na področju UI. Ponudnik bi moral pri opredeljevanju najustreznejših ukrepov za obvladovanje tveganja dokumentirati in pojasniti sprejete odločitve ter po potrebi vključiti strokovnjake in zunanje deležnike. Pri identifikaciji razumno predvidljive napačne uporabe visoko tveganih sistemov UI bi moral ponudnik zajeti uporabe sistemov UI, za katere se kljub temu, da niso neposredno zajete s predvidenim namenom in določene v navodilih za uporabo, lahko razumno pričakuje, da bodo posledica enostavno predvidljivega človeškega vedenja v okviru posebnih značilnosti in uporabe določenega sistema UI. Vse znane ali predvidljive okoliščine, povezane z uporabo visokotveganega sistema UI v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, ki lahko povzročijo tveganja za zdravje in varnost ali temeljne pravice, bi morale biti vključene v navodila za uporabo, ki jih zagotovi ponudnik. S tem se zagotovi, da je uvajalec seznanjen z njimi in jih upošteva pri uporabi visokotveganega sistema UI. Pri opredeljevanju in izvajanju ukrepov za zmanjšanje tveganja za predvidljivo napačno uporabo na podlagi te uredbe ponudnik v okviru obravnavanja predvidljive napačne uporabe ne bi smel zahtevati posebnega dodatnega učenja za visokotvegani sistem UI. Vendar se ponudnike spodbuja, naj po potrebi in če je to ustrezno razmislijo o takih dodatnih ukrepih za učenje, da bi ublažili razumno predvidljive napačne uporabe.

- (66) Za visokotvegane sisteme UI bi morale veljati zahteve glede obvladovanja tveganja, kakovosti in relevantnosti uporabljenih naborov podatkov, tehnične dokumentacije in vodenja evidenc, preglednosti in zagotavljanja informacij uvajalcem, človekovega nadzora ter robustnosti, točnosti in varnosti. Te zahteve so potrebne za učinkovito zmanjšanje tveganj za zdravje, varnost in temeljne pravice. Ker ni v razumni meri na voljo drugih manj omejevalnih ukrepov za trgovino, te zahteve ne predstavljajo neupravičene omejitve trgovine.

- (67) Visokokakovostni podatki in dostop do njih imajo ključno vlogo pri zagotavljanju strukture in zmogljivosti številnih sistemov UI, zlasti kadar se uporabljajo tehnike, ki vključujejo učenje modelov, s katerim bi zagotovili, da bo visokotvegani sistem UI deloval, kot je predvideno, in varno ter da ne bo postal vir diskriminacije, ki je prepovedana s pravom Unije. Visokokakovostni nabori učnih, testnih in validacijskih podatkov zahtevajo izvajanje ustreznih prakse vodenja in upravljanja podatkov. Nabori učnih, testnih in validacijskih podatkov, vključno z oznakami, bi morali biti ustrezni, dovolj reprezentativni in v največji možni meri brez napak in popolni glede na predvideni namen. Da bi olajšali skladnost s pravom Unije o varstvu podatkov, kot je Uredba (EU) 2016/679, bi morale prakse vodenja in upravljanja podatkov v primeru osebnih podatkov vključevati preglednost prvotnega namena zbiranja podatkov. Nabori podatkov bi morali imeti tudi ustrezne statistične lastnosti, tudi kar zadeva osebe ali skupine oseb, v zvezi s katerimi naj bi se uporabljal visokotvegani sistem UI, s posebnim poudarkom na zmanjševanju morebitnih pristranskosti v naborih podatkov, ki bi lahko vplivale na zdravje in varnost oseb, negativno vplivale na temeljne pravice ali povzročile diskriminacijo, prepovedano na podlagi prava Unije, zlasti kadar izhodni podatki vplivajo na vhodne podatke za prihodnje operacije (povratne zanke). Na primer, pristranskost je lahko inherentno prisotna v osnovnih naborih podatkov, zlasti kadar se uporabljajo pretekli podatki, ali se ustvari, ko se sistemi izvajajo v realnih razmerah.

Takšna inherentna pristranskost bi lahko vplivala na rezultate sistemov UI in se tudi običajno postopoma povečuje, zaradi česar se ohranja in povečuje tudi obstoječa diskriminacija, zlasti za osebe, ki pripadajo določenim ranljivim skupinam, vključno z rasnimi ali etničnimi skupinami. Zahteva, da morajo biti nabori podatkov čim bolj popolni in brez napak, ne bi smela vplivati na uporabo tehnik za ohranjanje zasebnosti v okviru razvoja in testiranja sistemov UI. Nabori podatkov morali zlasti v obsegu, ki ga zahteva njihov predvideni namen, upoštevati lastnosti, značilnosti ali elemente, ki so značilni za določeno geografsko, kontekstualno, vedenjsko ali funkcionalno okolje, v katerem naj bi se uporabljal sistem UI. Zahteve v zvezi z upravljanjem podatkov se lahko izpolnijo s pomočjo tretjih oseb, ki ponujajo certificirane storitve zagotavljanja skladnosti s predpisi, vključno s preverjanjem upravljanja podatkov, celovitosti nabora podatkov, praks učenja, validacije in testiranja podatkov, če je zagotovljena skladnost z zahtevami glede podatkov iz te uredbe.

- (68) Za razvoj in ocenjevanje visokotveganih sistemov UI bi morali imeti nekateri akterji, kot so ponudniki, priglašeni organi in drugi ustrezni subjekti, kot evropska vozlišča za digitalne inovacije, centri za testiranje in eksperimentiranje ter raziskovalci, možnost dostopa do visokokakovostnih naborov podatkov in njihove uporabe na ustreznih področjih dejavnosti, povezanih s to uredbo. Evropski skupni podatkovni prostori, ki jih je vzpostavila Komisija, ter olajšanje souporabe podatkov med podjetji in z vlado v javnem interesu bodo bistveni za zagotavljanje zaupanja vrednega, odgovornega in nediskriminatornega dostopa do visokokakovostnih podatkov za učenje, potrjevanje in testiranje sistemov UI. Evropski zdravstveni podatkovni prostor bo na področju zdravja na primer olajšal nediskriminatoren dostop do zdravstvenih podatkov in učenje algoritmov UI na teh naborih podatkov na varen, pravočasen, pregleden in zaupanja vreden način ter z ustreznim institucionalnim upravljanjem. Ustrezni pristojni organi, vključno s sektorskimi, ki zagotavljajo ali podpirajo dostop do podatkov, lahko podpirajo tudi zagotavljanje visokokakovostnih podatkov za učenje, validacijo in testiranje sistemov UI.
- (69) Pravica do zasebnosti in varstva osebnih podatkov mora biti zagotovljena v celotni življenjski dobi sistema UI. V zvezi s tem se pri obdelavi osebnih podatkov uporabljata načeli najmanjšega obsega podatkov ter vgrajenega in privzetega varstva podatkov, kot sta določeni v pravu Unije o varstvu podatkov. Ukrepi, ki jih ponudniki sprejmejo za zagotovitev skladnosti s temi načeli, lahko vključujejo ne le anonimizacijo in šifriranje, temveč tudi uporabo tehnologije, ki omogoča vnos algoritmov v podatke in učenje sistemov UI brez prenosa med stranmi ali kopiranja samih neobdelanih ali strukturiranih podatkov in brez poseganja v zahteve glede upravljanja podatkov iz te uredbe.

- (70) Da bi zaščitili pravico drugih pred diskriminacijo, ki bi lahko nastala zaradi pristranskosti v sistemih UI, bi morali imeti ponudniki možnost, da izjemoma, če je to nujno potrebno za zagotavljanje odkrivanja in popravljanja pristranskosti v zvezi z visokotveganimi sistemi UI, ob upoštevanju ustreznih zaščitnih ukrepov za temeljne pravice in svoboščine fizičnih oseb ter ob uporabi vseh veljavnih pogojev iz te uredbe ter pogojev iz uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktive (EU) 2016/680, obdelujejo tudi posebne kategorije osebnih podatkov kot zadevo bistvenega javnega interesa v smislu člena 9(2), točka (g), Uredbe (EU) 2016/679 in člena 10(2), točka (g), Uredbe (EU) 2018/1725.
- (71) Razumljive informacije o tem, kako so bili visokotvegani sistemi UI razviti in kako delujejo skozi celotno življenjsko dobo, so bistvene za omogočanje sledljivosti teh sistemov, preverjanje skladnosti z zahtevami iz te uredbe ter spremljanje njihovega delovanja in spremljanje po dajanju na trg. To zahteva vodenje evidenc in razpoložljivost tehnične dokumentacije, ki vsebuje informacije, potrebne za oceno skladnosti sistema UI z ustreznimi zahtevami in olajšanje spremljanja po dajanju na trg. Takšne informacije bi morale vključevati splošne značilnosti, zmogljivosti in omejitve sistema, uporabljene algoritme, podatke, postopke učenja, testiranja in potrjevanja ter dokumentacijo o ustreznem sistemu obvladovanja tveganja in biti pripravljene v jasni in celoviti obliki. Tehnično dokumentacijo bi bilo treba ustrezno posodabljati v celotni življenjski dobi sistema UI. Poleg tega bi morali visokotvegani sistemi UI tehnično omogočati samodejno beleženje dogodkov z dnevniki v celotni življenjski dobi sistema.

- (72) Pri reševanju problemov v zvezi z nepreglednostjo in kompleksnostjo nekaterih sistemov UI ter za pomoč uvajalcem pri izpolnjevanju njihovih obveznosti iz te uredbe bi bilo treba za visokotvegane sisteme UI zahtevati preglednost, preden se dajo na trg ali v uporabo. Visokotvegani sistemi UI bi morali biti zasnovani tako, da bi uvajalci lahko razumeli, kako sistem UI deluje, ocenili njegovo funkcionalnost ter razumeli njegove prednosti in omejitve. Visokotveganim sistemom UI bi morale biti priložene ustrezne informacije v obliki navodil za uporabo. Takšne informacije bi morale vključevati značilnosti, zmogljivosti in omejitve zmogljivosti sistema UI. Ti naj bi zajemali informacije o morebitnih znanih in predvidljivih okoliščinah, povezanih z uporabo visokotveganega sistema UI, vključno z ukrepi uvajalcev, ki lahko vplivajo na vedenje in zmogljivost sistema, v katerih lahko sistem UI povzroči tveganja za zdravje, varnost in temeljne pravice, o spremembah, ki jih je ponudnik vnaprej določil in ocenil glede skladnosti, ter o ustreznih ukrepih za človeški nadzor, vključno z ukrepi za lažjo razlago izhodnih podatkov sistema UI s strani uvajalcev. Preglednost, vključno s priloženimi navodili za uporabo, bi morala pomagati uvajalcem pri uporabi sistema in sprejemanju informiranih odločitev. Uvajalci bi morali biti med drugim v boljšem položaju za pravilno izbiro sistema, ki ga nameravajo uporabljati glede na obveznosti, ki veljajo zanje, biti poučeni o nameravani in izključeni uporabi ter pravilno in ustrezno uporabljati sistem UI. Da bi izboljšali čitljivost in dostopnost informacij, vključenih v navodila za uporabo, bi bilo treba, kadar je ustrezno vključiti ponazoritvene primere, na primer glede omejitev ter predvidene in izključene uporabe sistema UI. Ponudniki bi morali zagotoviti, da vsa dokumentacija, vključno z navodili za uporabo, vsebuje smiselne, celovite, dostopne in razumljive informacije, ob upoštevanju potreb in predvidljivega znanja ciljnih uvajalcev. Navodila za uporabo bi morala biti na voljo v jeziku, ki ga določi zadevna država članica in ga ciljni uvajalci brez težav razumejo.

- (73) Visokotvegani sistemi UI bi morali biti zasnovani in razviti tako, da lahko fizične osebe nadzorujejo njihovo delovanje, zagotavljajo, da se uporabljajo, kot je bilo predvideno, in da se njihovi vplivi obravnavajo v celotnem življenjskem ciklu sistema. V ta namen bi moral ponudnik sistema pred dajanjem sistema na trg ali v uporabo določiti ustrezne ukrepe za človeški nadzor. Zlasti bi morali taki ukrepi, kadar je primerno, zagotavljati, da za sistem veljajo vgrajene operativne omejitve, ki jih sistem sam ne more razveljaviti, da se sistem odziva na človeškega operaterja ter da imajo fizične osebe, ki jim je bil dodeljen človekov nadzor, potrebne kompetence, usposobljenost in pooblastila za opravljanje te vloge. Prav tako je bistveno po potrebi zagotoviti, da visokotvegani sistemi UI vključujejo mehanizme za usmerjanje in obveščanje fizične osebe, ki ji je bil dodeljen človeški nadzor, za sprejemanje informiranih odločitev o tem, ali, kdaj in kako posredovati, da bi se izognili negativnim posledicam ali tveganjem, ali ustaviti sistem, če ne deluje, kot je bilo predvideno. Glede na pomembne posledice, ki jih napačno ujemanje v nekaterih sistemih za biometrično identifikacijo ljudi pomeni za osebe, je za te sisteme ustrezno določiti okrepljeno zahtevo po človekovem nadzoru, tako da uvajalec ne more sprejeti ukrepa ali odločitve na podlagi identifikacije, ki izhaja iz sistema, če tega nista ločeno preverili in potrdili vsaj dve fizični osebi. Ti osebi sta lahko iz enega ali več subjektov in vključujeta osebo, ki upravlja ali uporablja sistem. Ta zahteva ne bi smela ustvariti nepotrebnega bremena ali zamud, in lahko bi zadoščalo, da bi se ločena preverjanja različnih oseb samodejno zabeležila v dnevnikih, ki jih ustvari sistem. Glede na posebnosti področij preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, nadzora meje in azila se ta zahteva ne bi smela uporabljati, kadar je v skladu s pravom Unije ali nacionalnim pravom uporaba te zahteve nesorazmerna.

- (74) Visokotvegani sistemi UI bi morali v celotni življenjski dobi delovati dosledno ter izpolnjevati ustrezno raven točnosti, robustnosti in kibernetske varnosti glede na njihov predvideni namen in v skladu s splošno priznanimi najsodobnejšimi tehnološkimi dosežki. Komisijo ter ustrezne organizacije in deležnike se spodbuja, naj ustrezno upoštevajo zmanjšanje tveganj in negativne učinke sistema UI. Pričakovano raven metrik zmogljivosti bi bilo treba navesti v priloženih navodilih za uporabo. Ponudniki so pozvani, naj te informacije sporočijo uvajalcem na jasn in lahko razumljiv način, brez nesporazumov ali zavajajočih izjav. Namen prava Unije o zakonskem meroslovju, vključno z direktivama 2014/31/EU³⁵ in 2014/32/EU³⁶ Evropskega parlamenta in Sveta, je zagotoviti točnost meritev ter prispevati k preglednosti in poštenosti trgovinskih poslov. V zvezi s tem bi morala Komisija v sodelovanju z ustreznimi deležniki in organizacijami, kot so organi za meroslovje in primerjalno analizo, po potrebi spodbujati razvoj referenčnih vrednosti in metodologij merjenja za sisteme UI. Pri tem bi se morala Komisija seznaniti z mednarodnimi partnerji, ki se ukvarjajo z meroslovjem in ustreznimi kazalniki merjenja v zvezi z UI, ter z njimi sodelovati.

³⁵ Direktiva 2014/31/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaj držav članic v zvezi z omogočanjem dostopnosti neavtomatskih tehtnic na trgu (UL L 96, 29.3.2014, str. 107).

³⁶ Direktiva 2014/32/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaj držav članic v zvezi z omogočanjem dostopnosti neavtomatskih tehtnic na trgu (UL L 96, 29.3.2014, str. 149).

- (75) Tehnična robustnost je ključna zahteva za visokotvegane sisteme UI. Morali bi biti odporni na škodljivo ali kako drugače nezaželeno ravnanje, ki je lahko posledica omejitev znotraj sistema ali okolja, v katerem sistem deluje (npr. napake, okvare, nedoslednosti, nepričakovane situacije). Zato bi bilo treba sprejeti tehnične in organizacijske ukrepe za zagotovitev odpornosti visokotveganih sistemov UI, na primer z zasnovo in razvojem ustreznih tehničnih rešitev za preprečevanje ali zmanjšanje škodljivega ali drugače nezaželenega vedenja. Takšne tehnične rešitve lahko na primer vključujejo mehanizme, ki sistemu omogočajo varno prekinitev delovanja (načrti varne odpovedi), če so prisotne določene nepravilnosti ali delovanje poteka zunaj določenih vnaprej določenih meja. Neuspešna zaščita pred temi tveganji bi lahko imela varnostne posledice ali negativno vplivala na temeljne pravice, na primer zaradi napačnih odločitev ali napačnih ali pristranskih izhodnih podatkov, ki jih ustvari sistem UI.
- (76) Kibernetška varnost ima ključno vlogo pri zagotavljanju odpornosti sistemov UI proti poskusom spreminjanja njihove uporabe, vedenja, zmogljivosti ali ogrožanja njihovih varnostnih lastnosti s strani zlonamernih tretjih oseb, ki izkoriščajo šibke točke sistema. Kibernetški napadi na sisteme UI lahko izkoristijo posebna sredstva UI, kot so nabori učnih podatkov (npr. zastrupitev podatkov) ali naučeni modeli (npr. nasprotovalni napadi ali sklepanje o članstvu), ali pa šibke točke digitalnih sredstev sistema UI ali osnovne infrastrukture IKT. Da bi zagotovili raven kibernetške varnosti, ki ustreza tveganjem, bi morali ponudniki visokotveganih sistemov UI sprejeti ustrezne ukrepe, kot je varnostni nadzor, in pri tem po potrebi tudi upoštevati osnovne infrastrukture IKT.

- (77) Brez poseganja v zahteve v zvezi z robustnostjo in natančnostjo iz te uredbe se lahko skladnost visokotveganih sistemov UI, ki spadajo na področje uporabe uredbe Evropskega parlamenta in Sveta o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi, v skladu z navedeno uredbo, z zahtevami glede kibernetске varnosti iz te uredbe dokaže z izpolnjevanjem bistvenih zahtev glede kibernetске varnosti iz navedene uredbe. Če visokotvegani sistemi UI izpolnjujejo bistvene zahteve iz uredbe o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi, štejejo za skladne z zahtevami glede kibernetске varnosti iz te uredbe, če je izpolnjevanje navedenih zahtev dokazano v EU izjavi o skladnosti ali delih izjave, izdane na podlagi navedene uredbe. V ta namen bi bilo treba pri oceni tveganj za kibernetско varnost, povezanih s proizvodom z digitalnimi elementi, razvrščenimi kot visokotvegani sistem UI v skladu s to uredbo, ki se izvede na podlagi uredbe o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi, upoštevati tveganja za kibernetско odpornost sistema UI na poskuse nepooblaščenih tretjih oseb, da z izkoriščanjem šibkih točk sistema spremenijo njegovo uporabo, vedenje ali zmogljivost, vključno s šibkimi točkami, ki so specifične za UI, kot so zastrupitev podatkov ali nasprotovalni napadi, ter v zvezi s tveganji za temeljne pravice, kot je zahtevano v tej uredbi.

- (78) Postopek ugotavljanja skladnosti iz te uredbe bi bilo treba uporabljati v zvezi z bistvenimi zahtevami glede kibernetске varnosti proizvoda z digitalnimi elementi, ki jih zajema uredba o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi in je razvrščen kot visokotvegani sistem UI na podlagi te uredbe. Vendar to pravilo ne bi smelo povzročiti znižanja potrebne ravni zanesljivosti za kritične proizvode z digitalnimi elementi, ki jih zajema uredba o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi. Zato z odstopanjem od tega pravila za visokotvegane sisteme UI, ki spadajo na področje uporabe te uredbe in so opredeljeni tudi kot pomembni in kritični proizvodi z digitalnimi elementi na podlagi uredbe o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi ter se zanje uporablja postopek ugotavljanja skladnosti na podlagi notranjega nadzora iz ene od prilog k tej uredbi, veljajo določbe o ugotavljanju skladnosti iz uredbe o horizontalnih zahtevah glede kibernetске varnosti za izdelke z digitalnimi elementi, kar zadeva bistvene zahteve glede kibernetске varnosti iz navedene uredbe. V tem primeru bi bilo treba za vse druge vidike, ki jih zajema ta uredba, uporabljati ustrezne določbe o ugotavljanju skladnosti na podlagi notranjega nadzora iz ene od prilog k tej uredbi. Komisija bi morala na podlagi poznavanja področja in strokovnega znanja agencije ENISA o politiki kibernetске varnosti in nalogah, dodeljenih agenciji ENISA na podlagi Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta³⁷, sodelovati z agencijo ENISA pri vprašanjih, povezanih s kibernetsko varnostjo sistemov UI.

³⁷ Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetске varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetски varnosti) (UL L 151, 7.6.2019, str. 15).

- (79) Primerno je, da določena fizična ali pravna oseba, opredeljena kot ponudnik, prevzame odgovornost za dajanje visokotveganega sistema UI na trg ali v uporabo, ne glede na to, ali je ta oseba tista, ki je zasnovala ali razvila sistem.
- (80) Kot podpisnice Konvencije Organizacije združenih narodov o pravicah invalidov so Unija in države članice pravno zavezane, da ščitijo invalide pred diskriminacijo in spodbujajo njihovo enakost, jim zagotovijo, da imajo enako kot drugi dostop do informacijskih in komunikacijskih tehnologij in sistemov, ter da se spoštuje njihova zasebnost. Ob vse večjem pomenu in uporabi sistemov UI bi morala uporaba načel univerzalnega oblikovanja pri vseh novih tehnologijah in storitvah zagotoviti popoln in enakopraven dostop vsem, ki so lahko izpostavljeni tehnologijam UI ali te tehnologije uporabljajo, tudi invalidom, na način, ki v celoti upošteva njihovo prirojeno dostojanstvo in raznolikost. Zato je bistvenega pomena, da ponudniki zagotavljajo popolno skladnost z zahtevami glede dostopnosti, tudi z Direktivo (EU) 2016/2102 Evropskega parlamenta in Sveta³⁸ in Direktivo (EU) 2019/882. Ponudniki bi morali zagotoviti skladnost s temi zahtevami že pri zasnovi. Zato bi bilo treba potrebne ukrepe v čim večji meri vključiti v zasnovo visokotveganega sistema UI.

³⁸ Direktiva (EU) 2016/2102 Evropskega parlamenta in Sveta z dne 26. oktobra 2016 o dostopnosti spletišč in mobilnih aplikacij organov javnega sektorja (UL L 327, 2.12.2016, str. 1).

- (81) Ponudnik bi moral vzpostaviti zanesljiv sistem upravljanja kakovosti, zagotoviti izvedbo zahtevanega postopka ugotavljanja skladnosti, pripraviti ustrezno dokumentacijo in vzpostaviti robusten sistem spremljanja po dajanju na trg. Ponudniki visokotveganih sistemov UI, za katere veljajo obveznosti v zvezi s sistemi upravljanja kakovosti na podlagi ustreznega sektorskega prava Unije, bi morali imeti možnost, da elemente sistema upravljanja kakovosti iz te uredbe vključijo v obstoječi sistem upravljanja kakovosti, določen v navedenem drugem sektorskem pravu Unije. Pri prihodnjih dejavnostih standardizacije ali smernicah, ki jih sprejme Komisija, bi bilo treba upoštevati tudi dopolnjevanje med to uredbo in obstoječim sektorskim pravom Unije. Javni organi, ki visokotvegane sisteme UI dajo v uporabo za lastno uporabo, lahko sprejmejo in izvajajo pravila za sistem upravljanja kakovosti kot del sistema upravljanja kakovosti, sprejetega bodisi na nacionalni ali na regionalni ravni, ob upoštevanju posebnosti sektorja ter pristojnosti in organizacije zadevnega javnega organa.

- (82) Da se omogoči izvajanje te uredbe in ustvarijo enaki konkurenčni pogoji za operaterje ter ob upoštevanju različnih oblik omogočanja dostopnosti digitalnih proizvodov, je pomembno zagotoviti, da lahko oseba s sedežem v Uniji v vseh okoliščinah organom zagotovi vse potrebne informacije o skladnosti sistema UI. Zato bi morali ponudniki s sedežem v tretjih državah pred dajanjem svojih sistemov UI na voljo v Uniji, s pisnim pooblastilom imenovati pooblaščenega zastopnika s sedežem v Uniji. Ta pooblaščen zastopnik ima ključno vlogo pri zagotavljanju skladnosti visokotveganih sistemov UI, ki jih ti ponudniki, ki nimajo sedeža v Uniji, dajejo na trg ali v uporabo v Uniji, in je njihova kontaktna oseba s sedežem v Uniji.
- (83) Glede na naravo in kompleksnost verige vrednosti za sisteme UI ter v skladu z novim zakonodajnim okvirom je bistveno zagotoviti pravno varnost in olajšati skladnost s to uredbo. Zato je treba pojasniti vlogo in posebne obveznosti zadevnih operaterjev v tej verigi vrednosti, kot so uvozniki in distributerji, ki lahko prispevajo k razvoju sistemov UI. V nekaterih situacijah bi lahko ti operaterji imeli več kot eno vlogo hkrati in bi morali zato kumulativno izpolnjevati vse zadevne obveznosti, povezane s temi vlogami. Tako bi na primer operater lahko hkrati bil distributer in uvoznik.

- (84) Za zagotovitev pravne varnosti je treba pojasniti, da bi bilo treba pod določenimi pogoji vsakega distributerja, uvoznika, uvajalca ali druge tretje osebe šteti za ponudnika visokotveganega sistema UI in bi zato moral prevzeti vse zadevne obveznosti. To bi veljalo, če ta stranka svoje ime ali znamko vnese v visokotvegani sistem UI, ki je že dan na trg ali v uporabo, brez poseganja v pogodbene dogovore, ki določajo, da se obveznosti dodelijo drugače. To bi veljalo tudi, če ta stranka bistveno spremeni visokotvegani sistem UI, ki je že bil dan na trg ali v uporabo, na način, da ostane visokotvegani sistem UI v skladu s to uredbo, ali če spremeni predvideni namen sistema UI, vključno z sistemom UI za splošne namene, ki ni bil razvrščen kot sistem visokega tveganja in je že bil dan na trg ali v uporabo, na način, da sistem UI postane sistem visokega tveganja v skladu s to uredbo. Te določbe bi bilo treba uporabljati brez poseganja v bolj specifične določbe v okviru določene harmonizacijske zakonodaje, temelječe na novem zakonodajnem okviru, ki naj bi se uporabljala skupaj s to uredbo. Na primer člen 16(2) Uredbe (EU) 2017/745, v katerem je določeno, da nekatere spremembe ne bi smele šteti kot spremembe pripomočka, ki bi lahko vplivale na skladnost z veljavnimi zahtevami, bi bilo treba še naprej uporabljati za visokotvegane sisteme UI, ki so medicinski pripomočki v smislu navedene uredbe.

- (85) Sistemi UI za splošne namene se lahko uporabljajo kot samostojni visokotvegani sistemi UI ali pa so komponente drugih visokotveganih sistemov UI. Zato bi morali ponudniki takih sistemov zaradi njihove posebne narave in za zagotovitev pravične delitve odgovornosti v verigi vrednosti UI ne glede na to, ali lahko drugi ponudniki te sisteme uporabljajo kot samostojne visokotvegane sisteme UI ali kot komponente visokotveganih sistemov UI in če v tej uredbi ni določeno drugače, tesno sodelovati s ponudniki zadevnih visokotveganih sistemov UI, da bi jim omogočili izpolnjevanje obveznosti iz te uredbe, in s pristojnimi organi, ustanovljenimi na podlagi te uredbe.
- (86) Kadar na podlagi pogojev iz te uredbe ponudnik, ki je sistem UI prvotno dal na trg ali v uporabo, za namene te uredbe ne bi smel več šteti za ponudnika in če ta ponudnik ni izrecno izključil spremembe sistema UI v visokotvegani sistem UI, bi moral nekdanji ponudnik kljub temu tesno sodelovati in dati na voljo potrebne informacije ter zagotoviti razumno pričakovani tehnični dostop in drugo pomoč, ki so potrebni za izpolnjevanje obveznosti iz te uredbe, zlasti v zvezi s skladnostjo visokotveganih sistemov UI z ugotavljanjem skladnosti.
- (87) Poleg tega, kadar visokotvegani sistem UI, ki je varnostna komponenta proizvoda, ki spada na področje uporabe harmonizacijske zakonodaje Unije na podlagi novega zakonodajnega okvira, ni dan na trg ali v uporabo neodvisno od proizvoda, bi moral proizvajalec proizvoda, opredeljen v navedeni zakonodaji, izpolnjevati obveznosti ponudnika iz te uredbe in zlasti zagotoviti, da sistem UI, vgrajen v končni proizvod, izpolnjuje zahteve iz te uredbe.

- (88) V verigi vrednosti UI sisteme UI, orodja in storitve, pa tudi komponente ali procese, ki jih ponudnik vključi v sistem UI z različnimi cilji, vključno z učenjem modelov, ponovnim učenjem modelov, testiranjem in ocenjevanjem modelov, vključevanjem v programsko opremo ali drugimi vidiki razvoja modela, pogosto dobavlja več strani. Te strani imajo pomembno vlogo v verigi vrednosti v odnosu do ponudnika visokotveganega sistema UI, v katerega so vključeni njihovi sistemi UI, orodja, storitve, komponente ali procesi, in bi morale temu ponudniku v pisni obliki zagotoviti potrebne informacije, zmogljivosti, tehnični dostop in drugo pomoč na podlagi splošno priznanih najsodobnejših tehnoloških dosežkov, da bi lahko ponudnik v celoti izpolnjeval obveznosti iz te uredbe, ne da bi bile pri tem ogrožene njegove pravice intelektualne lastnine ali poslovne skrivnosti.
- (89) Za tretje osebe, ki javnosti omogočajo dostop do orodij, storitev, postopkov ali komponent UI, ki niso modeli UI za splošne namene, ne bi smela veljati obveznost glede izpolnjevanja zahtev, ki se nanašajo na odgovornosti v verigi vrednosti UI, zlasti do ponudnika, ki jih je uporabil ali vključil, če so ta orodja, storitve, postopki ali komponente UI dostopni na podlagi proste in odprtokodne licence. Razvijalce brezplačnih in odprtokodnih orodij, storitev, postopkov ali komponent UI, ki niso modeli UI za splošne namene, pa bi bilo treba spodbujati k izvajanju splošno sprejetih dokumentacijskih praks, kot so vzorčne kartice in podatkovni listi, da bi pospešili izmenjavo informacij v verigi vrednosti UI, kar bi omogočilo spodbujanje zaupanja vrednih sistemov UI v Uniji.

- (90) Komisija bi lahko razvila in priporočila prostovoljne vzorčne pogodbene pogoje med ponudniki visokotveganih sistemov UI in tretjimi osebami, ki zagotavljajo orodja, storitve, komponente ali procese, ki se uporabljajo ali vključujejo v visokotvegane sisteme UI, da bi olajšali sodelovanje v verigi vrednosti. Komisija bi morala pri oblikovanju prostovoljnih vzorčnih pogodbenih pogojev upoštevati morebitne pogodbene zahteve, ki se uporabljajo v posameznih sektorjih ali poslovnih primerih.
- (91) Glede na naravo sistemov UI ter tveganja za varnost in temeljne pravice, ki so morda povezana z njihovo uporabo, tudi kar zadeva potrebo po zagotovitvi ustreznega spremljanja zmogljivosti sistema UI v realnem življenju, je primerno določiti posebne odgovornosti za uvajalce. Uvajalci bi morali zlasti sprejeti ustrezne tehnične in organizacijske ukrepe za zagotovitev, da uporabljajo visokotvegane sisteme UI v skladu z navodili za uporabo, pri čemer bi bilo treba določiti nekatere druge obveznosti v zvezi s spremljanjem delovanja sistemov UI in v zvezi z vodenjem evidenc, če je to primerno. Poleg tega bi morali uvajalci zagotoviti, da imajo osebe, dodeljene za izvajanje navodil za uporabo in človeški nadzor, kot je določeno v tej uredbi, potrebne kompetence, zlasti ustrezno raven pismenosti, usposobljenosti in pooblastil na področju UI za pravilno izpolnjevanje teh nalog. Te obveznosti ne bi smele posegati v druge obveznosti uvajalcev v zvezi z visokotveganimi sistemi UI na podlagi prava Unije ali nacionalnega prava.

- (92) Ta uredba ne posega v obveznosti delodajalcev, da delavce ali njihove predstavnike obveščajo ali se z njimi posvetujejo na podlagi prava Unije ali nacionalnega prava in prakse, vključno z Direktivo 2002/14/ES Evropskega parlamenta in Sveta³⁹ o odločitvah o dajanju v uporabo ali uporabi sistemov UI. Še naprej je treba zagotavljati informacije delavcem in njihovim predstavnikom o načrtovani uvedbi visokotveganih sistemov UI na delovnem mestu, kadar niso izpolnjeni pogoji za te obveznosti glede obveščanja ali obveščanja in posvetovanja iz drugih pravnih instrumentov. Poleg tega je taka pravica do obveščenosti pomožna in potrebna za cilj varstva temeljnih pravic, na katerem temelji ta uredba. Zato bi bilo treba v tej uredbi določiti zahtevo po informacijah v ta namen, ne da bi to vplivalo na obstoječe pravice delavcev.

³⁹ Direktiva 2002/14/ES Evropskega parlamenta in Sveta z dne 11. marca 2002 o določitvi splošnega okvira za obveščanje in posvetovanje z delavci v Evropski skupnosti (UL L 80, 23.3.2002, str. 29).

- (93) Poleg tega, da lahko tveganja, povezana s sistemi UI, nastanejo zaradi načina zasnove takih sistemov, lahko tveganja izvirajo tudi iz tega, kako se taki sistemi uporabljajo. Uvajalci visokotveganega sistema UI imajo zato ključno vlogo pri skrbi za zaščito temeljnih pravic, kar dopolnjuje obveznosti ponudnika pri razvoju sistema UI. Uvajalci najbolj razumejo, kako se bo visokotvegani sistem UI dejansko uporabljal, in lahko tako opredelijo potencialna velika tveganja, ki niso bila predvidena v fazi razvoja, saj natančneje poznajo okoliščine uporabe, osebe ali skupine oseb, ki bodo verjetno izpostavljene, vključno z ranljivimi skupinami. Uvajalci visokotveganih sistemov UI, navedeni v eni od prilog k tej uredbi, imajo tudi ključno vlogo pri obveščanju fizičnih oseb in bi morali pri sprejemanju odločitev ali pomoči pri sprejemanju odločitev v zvezi s fizičnimi osebami po potrebi obvestiti fizične osebe, da se zanje uporablja visokotvegani sistem UI. Te informacije bi morale vključevati njegov predvideni namen in vrsto odločitev, ki jih sprejema. Uvajalec bi moral fizične osebe obvestiti tudi o njihovi pravici do obrazložitve iz te uredbe. Kar zadeva visokotvegane sisteme UI, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, bi bilo treba to obveznost izvajati v skladu s členom 13 Direktive (EU) 2016/680.

- (94) Vsaka obdelava biometričnih podatkov, vključena v uporabo sistemov UI za biometrično identifikacijo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, mora biti skladna s členom 10 Direktive (EU) 2016/680, ki omogoča tako obdelavo le, kadar je to nujno potrebno, ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, in kadar je to dovoljeno v skladu s pravom Unije ali pravom države članice. Kadar je taka uporaba odobrena, je treba spoštovati tudi načela iz člena 4(1) Direktive (EU) 2016/680, vključno z zakonitostjo, pravičnostjo in preglednostjo, omejitvijo namena, točnostjo in omejitvijo shranjevanja.
- (95) Brez poseganja v veljavno pravo Unije, zlasti v Uredbo (EU) 2016/679 in Direktivo (EU) 2016/680, in ob upoštevanju intruzivne narave sistemov za naknadno biometrično identifikacijo na daljavo, bi bilo treba za uporabo sistemov za naknadno biometrično identifikacijo na daljavo uporabljati zaščitne ukrepe. Sisteme za naknadno biometrično identifikacijo na daljavo bi bilo treba vedno uporabljati na način, ki je sorazmeren, zakonit in nujno potreben ter tako ciljno usmerjen v smislu posameznikov, ki jih je treba identificirati, lokacije, časovnega obsega in na podlagi zaprtega nabora podatkov iz zakonito pridobljenih videoposnetkov. V nobenem primeru sistemov za naknadno biometrično identifikacijo na daljavo ne bi smeli uporabljati v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, da ne bi povzročili neselektivnega nadzora. Pogoji za naknadno biometrično identifikacijo na daljavo v nobenem primeru ne bi smeli biti podlaga za izogibanje pogojem prepovedi in strogim izjemam za biometrično identifikacijo na daljavo v realnem času.

- (96) Da bi učinkovito zagotovili varstvo temeljnih pravic, bi morali uvajalci visokotveganih sistemov UI, ki so osebe javnega prava, ali zasebni subjekti, ki zagotavljajo javne storitve, in uvajalci, ki uporabljajo nekatere visokotvegane sisteme UI, navedene v eni od prilog k tej uredbi, kot so bančni ali zavarovalniški subjekti, pred začetkom uporabe izvesti oceno učinka na temeljne pravice. Storitve, pomembne za posameznike, ki so javne narave, lahko zagotavljajo tudi zasebni subjekti. Zasebni subjekti, ki zagotavljajo takšne javne storitve, so povezani z nalogami v javnem interesu, na primer na področjih izobraževanja, zdravstvenega varstva, socialnih storitev, stanovanj in razsojanja. Cilj ocene učinka na temeljne pravice je, da uvajalec opredeli posebna tveganja za pravice posameznikov ali skupin posameznikov, ki bodo verjetno izpostavljene, in ukrepe, ki jih je treba sprejeti v primeru uresničitve teh tveganj. Oceno učinka bi bilo treba opraviti pred uvedbo visokotvegane sistema UI in bi jo bilo treba posodobiti, kadar uvajalec meni, da se je spremenil kateri od pomembnih dejavnikov. V oceni učinka bi bilo treba opredeliti ustrezne procese uvajalca, v katerih se bo visokotvegani sistem UI uporabljal v skladu s predvidenim namenom, ter opis obdobja in pogostosti uporabe sistema ter posebnih kategorij fizičnih oseb in skupin, ki bodo verjetno izpostavljene v posebnih okoliščinah uporabe.

Ocena bi morala vključevati tudi opredelitev posebnih tveganj škode, ki bi lahko vplivala na temeljne pravice teh oseb ali skupin. Da bi zagotovili pravilno izvedbo te ocene učinka, bi moral uvajalec pri njenem izvajanju upoštevati ustrezne informacije, med drugim tudi tiste, ki jih ponudnik visokotveganega sistema UI navede v navodilih za uporabo. Glede na ugotovljena tveganja bi morali uvajalci določiti ukrepe, ki jih je treba sprejeti v primeru uresničitve teh tveganj, vključno na primer z ureditvami upravljanja v tem posebnem okviru uporabe, kot so ureditve za človeški nadzor v skladu z navodili za uporabo ali obravnavanje pritožb in postopki pravnega varstva, saj bi lahko bili ključni za zmanjšanje tveganj za temeljne pravice v konkretnih primerih uporabe. Po izvedbi te ocene učinka bi moral uvajalec o tem obvestiti ustrezni organ za nadzor trga. Za zbiranje ustreznih informacij, potrebnih za izvedbo ocene učinka, bi lahko uvajalci visokotveganega sistema UI, zlasti kadar se sistemi UI uporabljajo v javnem sektorju, v izvajanju takih ocen učinka in oblikovanje ukrepov, ki jih je treba sprejeti v primeru uresničitve tveganj, po potrebi vključili ustrezne deležnike, vključno s predstavniki skupin oseb, na katere bo sistem UI verjetno vplival, neodvisne strokovnjake in organizacije civilne družbe. Evropski urad za umetno inteligenco (v nadaljnjem besedilu: Urad za UI) bi moral pripraviti predlogo vprašalnika, da bi olajšali skladnost in zmanjšali upravno breme za uvajalce.

- (97) Da bi omogočili pravno varnost, bi moral biti pojem modelov UI za splošne namene jasno opredeljen in ločen od pojma sistemov UI. Opredelitev bi morala temeljiti na ključnih funkcionalnih značilnostih modela UI za splošne namene, zlasti na splošnosti in sposobnosti opravljanja širokega nabora različnih nalog. Ti modeli se običajno učijo s pomočjo velikih količin podatkov z različnimi metodami, kot so samonadzorovano, nenadzorovano ali okrepljeno učenje. Modeli UI za splošne namene se lahko dajo na trg na različne načine, tudi prek knjižnic, vmesnikov za aplikacijsko programiranje (API), kot neposredni prenos ali kot fizična kopija. Ti modeli se lahko dodatno spremenijo ali prilagodijo novim modelom. Čeprav so modeli UI bistvene komponente sistemov UI, sami po sebi niso sistemi UI. Da bi modeli UI postali sistemi UI, jim je treba dodati dodatne komponente, kot je na primer uporabniški vmesnik. Modeli UI so običajno vključeni v sisteme UI in so njihov sestavni del. V tej uredbi so določena posebna pravila za modele UI za splošne namene in modele UI za splošne namene, ki predstavljajo sistemska tveganja, ki bi jih bilo treba uporabljati tudi, kadar so ti modeli vključeni v sistem UI ali tvorijo del sistema UI. Razumeti bi bilo treba, da bi bilo treba obveznosti ponudnikov modelov UI za splošne namene uporabljati, ko bodo ti modeli dani na trg.

Če ponudnik modela UI za splošne namene vključi lastni model v svoj sistem UI, ki je dostopen na trgu ali je v uporabi, bi bilo treba šteti, da je ta model dan na trg, zato bi bilo treba še naprej uporabljati obveznosti iz te uredbe za modele, poleg tistih za sisteme UI. Obveznosti, ki so določene za modele, se v nobenem primeru ne bi smeli uporabljati, če se lastni model uporablja za izključno notranje postopke, ki niso bistveni za zagotavljanje proizvoda ali storitve tretjim osebam, in to ne vpliva na pravice fizičnih oseb. Glede na njihove morebitne znatne negativne učinke bi morale za modele UI za splošne namene s sistemskim tveganjem vedno veljati ustrezne obveznosti iz te uredbe. Opredelitev ne bi smela zajemati modelov UI, ki se uporabljajo pred dajanjem na trg izključno za namene raziskav, razvoja in izdelave prototipov. To ne posega v obveznost skladnosti s to uredbo, kadar se po takšnih dejavnostih model da na trg.

- (98) Medtem ko bi bilo mogoče splošnost modela med drugim določiti tudi s številnimi parametri, bi bilo treba šteti, da modeli z vsaj milijardo parametrov in naučeni z veliko količino podatkov, ki uporabljajo samonadzor v velikem obsegu, kažejo znatno splošnost in so sposobni kompetentno opravljati širok nabor različnih nalog.
- (99) Veliki generativni modeli UI so tipičen primer modela UI za splošne namene, saj omogočajo prilagodljivo ustvarjanje vsebin, kot so besedilo, zvočni zapisi, slike ali videoposnetki, ki se lahko zlahka prilagodijo širokemu spektru različnih nalog.

- (100) Kadar je model UI za splošne namene vključen v sistem UI ali je del sistema UI, bi bilo treba ta sistem šteti za sistem UI za splošne namene, če se lahko zaradi te vključitve ta sistem uporablja za različne namene. Sistem UI za splošne namene se lahko uporablja neposredno ali pa se lahko vključi v druge sisteme UI.
- (101) Ponudniki modelov UI za splošne namene imajo posebno vlogo in odgovornost vzdolž verige vrednosti UI, saj so lahko modeli, ki jih zagotavljajo, podlaga za vrsto sistemov nižje v verigi, ki jih pogosto zagotavljajo ponudniki nižje v verigi, ki potrebujejo dobro razumevanje modelov in njihovih zmogljivosti, da bi omogočili vključitev takih modelov v njihove proizvode in izpolnili svoje obveznosti iz te uredbe ali drugih predpisov. Zato bi bilo treba določiti sorazmerne ukrepe za preglednost, vključno s pripravo in posodabljanjem dokumentacije ter zagotavljanjem informacij o modelu UI za splošne namene, ki ga lahko uporabljajo ponudniki nižje v verigi. Ponudnik modela UI za splošne namene bi moral pripraviti in posodabljati tehnično dokumentacijo, da bi jo na zahtevo dal na voljo Uradu za UI in pristojnim nacionalnim organom. Minimalni sklop elementov, ki jih je treba vključiti v tako dokumentacijo, bi bilo treba določiti v posebnih prilogah k tej uredbi. Na Komisijo bi bilo treba prenesti pooblastilo za spreminjanje navedenih prilog z delegiranimi akti glede na hiter tehnološki razvoj.

- (102) Programska oprema in podatki, vključno z modeli, objavljenimi na podlagi proste in odprtokodne licence, ki omogoča njihovo prosto izmenjavo in če uporabniki lahko prosto dostopajo do njih ali njihovih spremenjenih različic, jih uporabljajo, spreminjajo in ponovno distribuirajo, lahko prispevajo k raziskavam in inovacijam na trgu ter gospodarstvu Unije zagotovijo znatne priložnosti za rast. Razmisliti bi bilo treba o modelih UI za splošne namene, objavljenih na podlagi prostih in odprtokodnih licenc, da bi zagotovili visoko raven preglednosti in odprtosti, če so njihovi parametri, vključno z utežmi, informacijami o arhitekturi modela in informacijami o uporabi modela, javno dostopni. Licenca bi morala šteti za prosto in odprtokodno, tudi kadar uporabnikom omogoča uporabo, kopiranje, distribucijo, preučevanje, spreminjanje in izboljševanje programske opreme in podatkov, vključno z modeli, pod pogojem, da se navede originalni ponudnik modela in da se upoštevajo enaki ali primerljivi pogoji distribucije.
- (103) Brezplačne in odprtokodne komponente UI zajemajo programsko opremo in podatke, vključno z modeli in modeli UI za splošne namene, orodji, storitvami ali procesi sistema UI. Brezplačne in odprtokodne komponente UI se lahko zagotovijo prek različnih kanalov, vključno z njihovim razvojem v odprtih odložiščih. Za namene te uredbe komponente UI, ki se zagotavljajo proti plačilu ali so kako drugače monetizirane, med drugim z zagotavljanjem tehnične podpore ali drugih storitev, tudi prek platforme programske opreme, povezane s komponento UI, ali z uporabo osebnih podatkov iz razlogov, ki niso izključno namenjeni izboljšanju varnosti, združljivosti ali interoperabilnosti programske opreme, z izjemo transakcij med mikropodjetji, ne bi smele biti upravičene do izjem, določenih za brezplačne in odprtokodne komponente UI. Dejstvo, da so komponente UI na voljo prek odprtih odložišč, samo po sebi ne bi smelo pomeniti monetizacije.

- (104) Za ponudnike modelov UI za splošne namene, ki se objavijo na podlagi proste in odprtokodne licence ter katerih parametri, vključno z utežmi, informacijami o arhitekturi modela in informacijami o uporabi modela, so javno dostopni, bi morale veljati izjeme v zvezi z zahtevami glede preglednosti, ki veljajo za modele UI za splošne namene, razen če lahko šteje, da predstavljajo sistemsko tveganje; v tem primeru okoliščina, da je model pregleden in ga spremlja odprtokodna licenca, ne bi smela šteti za zadosten razlog za izključitev izpolnjevanja obveznosti iz te uredbe. V vsakem primeru pa glede na to, da objava modelov UI za splošne namene v okviru proste in odprtokodne licence ne razkrije nujno bistvenih informacij o naboru podatkov, ki se uporablja za učenje ali izpopolnjevanje modela, in o tem, kako je bila s tem zagotovljena skladnost z avtorskim pravom, se izjema, določena za modele UI za splošne namene, od skladnosti z zahtevami, povezanimi s preglednostjo, ne bi smela nanašati na obveznost priprave povzetka vsebine, ki se uporablja za učenje modelov, in obveznost vzpostavitve politike za skladnost z avtorskim pravom Unije, zlasti za opredelitev in skladnost s pridržkom pravic na podlagi člena 4(3) Direktive (EU) 2019/790 Evropskega parlamenta in Sveta⁴⁰.

⁴⁰ Direktiva (EU) 2019/790 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o avtorski in sorodnih pravicah na enotnem digitalnem trgu in spremembi direktiv 96/9/ES in 2001/29/ES (UL L 130, 17.5.2019, str. 92).

- (105) Modeli UI za splošne namene, zlasti veliki generativni modeli UI, ki lahko ustvarijo besedilo, slike in druge vsebine, predstavljajo edinstvene priložnosti za inovacije, pa tudi izzive za umetnike, avtorje in druge ustvarjalce ter njihov način ustvarjanja, razširjanja, uporabe in koriščenja njihovih ustvarjalnih vsebin. Za razvoj in učenje takih modelov je potreben dostop do velikih količin besedil, slik, videoposnetkov in drugih podatkov. Za pridobivanje in analizo takih vsebin, ki so lahko zaščitene z avtorskimi in sorodnimi pravicami, se lahko v tem kontekstu obsežno uporabljajo tehnike besedilnega in podatkovnega rudarjenja. Za vsako uporabo avtorsko zaščitene vsebin je potrebno dovoljenje zadevnega imetnika pravic, razen če se uporabljajo ustrezne izjeme in omejitve avtorskih pravic. Z Direktivo (EU) 2019/790 so bile uvedene izjeme in omejitve, ki pod določenimi pogoji omogočajo reprodukcije in izvlečke del ali drugih zaščitene predmetov za namene besedilnega in podatkovnega rudarjenja. Na podlagi teh pravil se lahko imetniki pravic odločijo, da bodo svoje pravice pridržali za svoja dela ali druge zaščitene predmete, da bi preprečili besedilno in podatkovno rudarjenje, razen če se to izvaja za namene znanstvenega raziskovanja. Kadar so pravice do izvzetja izrecno in na ustrezen način pridržane, morajo ponudniki modelov UI za splošne namene pridobiti dovoljenje imetnikov pravic, če želijo v zvezi s takimi deli izvajati besedilno in podatkovno rudarjenje.

- (106) Ponudniki, ki dajejo modele UI za splošne namene na trg Unije, bi morali zagotoviti skladnost z ustreznimi obveznostmi iz te uredbe. V ta namen bi morali ponudniki modelov UI za splošne namene vzpostaviti politiko za skladnost s pravom Unije o avtorskih in sorodnih pravicah, zlasti za opredelitev pridržka pravic, ki jih izrazijo imetniki pravic na podlagi člena 4(3) Direktive (EU) 2019/790, in skladnost z njim. Vsak ponudnik, ki daje model UI za splošne namene na trg Unije, bi moral to obveznost izpolnjevati ne glede na jurisdikcijo, v kateri se izvajajo dejanja, povezana z avtorskimi pravicami, na katerih temelji učenje teh modelov UI za splošno rabo. To je potrebno za zagotovitev enakih konkurenčnih pogojev med ponudniki modelov UI za splošne namene, pri čemer noben ponudnik ne bi smel imeti konkurenčne prednosti na trgu Unije z uporabo standardov avtorskih pravic, ki so nižji od standardov, določenih v Uniji.

- (107) Da bi izboljšali preglednost podatkov, ki se uporabljajo pri predhodnem učenju in učenju modelov UI za splošne namene, vključno z besedilom in podatki, zaščitenimi z avtorskim pravom, je ustrezno, da ponudniki takih modelov pripravijo in objavijo dovolj podroben povzetek vsebine, ki se uporablja za učenje modela UI za splošne namene. Upoštevajoč potrebo po varovanju poslovnih skrivnosti in zaupnih poslovnih informacij bi moral biti ta povzetek v svojem področju uporabe na splošno izčrpen in ne tehnično podroben, da bi strankam z zakonitimi interesi, vključno z imetniki avtorskih pravic, olajšali uveljavljanje in izvajanje njihovih pravic na podlagi prava Unije, na primer z navedbo glavnih zbirk podatkov ali naborov podatkov, ki so bili uporabljeni pri učenju, kot so velike zasebne ali javne podatkovne zbirke ali podatkovni arhivi, ter z opisno razlago drugih uporabljenih virov podatkov. Primerno je, da Urad za UI zagotovi predlogo za povzetek, ki bi moral biti preprost in učinkovit ter ponudniku omogočiti, da zagotovi zahtevani povzetek v opisni obliki.
- (108) Kar zadeva obveznosti ponudnikov modelov UI za splošne namene, da vzpostavijo politiko za skladnost z avtorskim pravom Unije in javno objavijo povzetek vsebine, uporabljene za učenje, bi moral Urad za UI spremljati, ali je ponudnik izpolnil te obveznosti brez preverjanja ali ocene učnih podatkov za vsak posamezen primer posebej z vidika njihove skladnosti z avtorskimi pravicami. Ta uredba ne vpliva na izvrševanje pravil o avtorskih pravicah, kot je določeno na podlagi prava Unije.

- (109) Izpolnjevanje obveznosti, ki veljajo za ponudnike modelov UI za splošne namene, bi moralo biti sorazmerno in primerno vrsti ponudnika modela, pri čemer bi bilo treba izključiti potrebo glede izpolnjevanja teh obveznosti za osebe, ki razvijajo ali uporabljajo modele za nepoklicne ali znanstvenoraziskovalne namene, vendar bi jih bilo treba kljub temu spodbujati k prostovoljnemu izpolnjevanju teh obveznosti. Brez poseganja v avtorsko pravo Unije bi bilo treba pri izpolnjevanju teh obveznosti ustrezno upoštevati velikost ponudnika in omogočiti poenostavljene načine izpolnjevanja obveznosti za MSP, vključno z zagonskimi podjetji, ki ne bi smeli predstavljati pretiranih stroškov in ne bi smeli odvrnati od uporabe takih modelov. V primeru spremembe ali izpopolnjevanja modela bi morale biti obveznosti ponudnikov modelov UI za splošne namene omejene na to spremembo ali izpopolnitev, na primer z dopolnitvijo že obstoječe tehnične dokumentacije z informacijami o spremembah, vključno z novimi viri učnih podatkov, da bi izpolnili obveznosti glede verige vrednosti iz te uredbe.

- (110) Modeli UI za splošne namene bi lahko predstavljali sistemska tveganja, ki med drugim vključujejo vse dejanske ali razumno predvidljive negativne učinke v zvezi z večjimi nesrečami, motnjami v kritičnih sektorjih ter resnimi posledicami za javno zdravje in varnost, vse dejanske ali razumno predvidljive negativne učinke na demokratične procese ter javno in gospodarsko varnost ter razširjanje nezakonitih, lažnih ali diskriminatornih vsebin. Sistemska tveganja bi bilo treba razumeti tako, da se povečujejo z zmogljivostmi in dosegom modela, da se lahko pojavijo v celotnem življenjskem ciklu modela in da nanje vplivajo pogoji napačne uporabe, zanesljivost modela, pravičnost modela in varnost modela, stopnja avtonomije modela, njegov dostop do orodij, novi ali kombinirani načini, strategije objave in distribucije, možnost odstranitve varovalnih mehanizmov in drugi dejavniki. V mednarodnih pristopih je bilo do zdaj zlasti ugotovljeno, da je treba pozornost nameniti tveganjem, ki izhajajo iz morebitne namerne napačne uporabe ali nenamernih problemov pri nadzoru v zvezi z usklajevanjem s človeškim namenom; kemičnim, biološkim, radiološkim in jedrskim tveganjem, kot so načini, kako zmanjšati vstopne ovire, vključno z razvojem orožja, nabavo njegove zasnove ali njegove uporabo; ofenzivnim kibernetiskim zmogljivostim, kot so načini, ki omogočajo odkrivanje, izkoriščanje ali operativno uporabo šibkih točk; učinkom interakcije in uporabe orodij, vključno na primer z zmogljivostjo za nadzor fizičnih sistemov in motenj v kritični infrastrukturi; tveganjem, povezanimi z modeli, ki izdelujejo kopije ali se „samoreplicirajo“ ali učijo druge modele; načinom, kako lahko modeli povzročijo škodljivo pristranskost in diskriminacijo, ker ustvarjajo tveganja za posameznike, skupnosti ali družbe; omogočanju dezinformacij ali ogrožanju zasebnosti z grožnjami demokratičnim vrednotam in človekovim pravicam; tveganju, da bi določen dogodek lahko povzročil verižno reakcijo z znatnimi negativnimi učinki, ki bi lahko vplivali na celo mesto, celotno domeno dejavnosti ali celotno skupnost.

- (111) Treba bi bilo določiti metodologijo za razvrstitev modelov UI za splošne namene kot modelov UI za splošne namene s sistemskimi tveganji. Ker sistemska tveganja izhajajo iz posebno visokih zmogljivosti, bi bilo treba za model UI za splošne namene šteti, da predstavlja sistemska tveganja, če ima zmogljivosti z visoko učinkovitostjo, ocenjene na podlagi ustreznih tehničnih orodij in metodologij, ali znaten vpliv na notranji trg zaradi svojega dosega. Zmogljivosti z visoko učinkovitostjo v modelih UI za splošne namene pomenijo zmogljivosti, ki so enake zmogljivostim, zabeleženim v najbolj naprednih modelih UI za splošne namene, ali jih presegajo. Celoten nabor zmogljivosti modela bi bilo mogoče bolje razumeti po tem, ko se da na trg ali ko so uvajalci v interakciji z modelom. V skladu z najsodobnejšimi tehnološkimi dosežki v času začetka veljavnosti te uredbe je kumulativni znesek izračuna, ki se uporablja za učenje modela UI za splošne namene, merjen z operacijami s plavajočo vejico, eden od ustreznih približkov za zmogljivosti modela. Kumulativni znesek izračuna, ki se uporablja za učenje, vključuje izračun, ki se uporablja za dejavnosti in metode, namenjene povečanju zmogljivosti modela pred uvedbo, kot so predhodno učenje, sintetično ustvarjanje podatkov in izpopolnjevanje. Zato bi bilo treba določiti začetni prag operacij s plavajočo vejico, ki, če ga doseže model UI za splošne namene, privede do domneve, da model šteje za model UI za splošne namene s sistemskimi tveganji. Ta prag bi bilo treba sčasoma prilagoditi, da bi odražal tehnološke in industrijske spremembe, kot so algoritemске izboljšave ali večja učinkovitost strojne opreme, dopolniti pa bi ga bilo treba z referenčnimi vrednostmi in kazalniki za zmogljivost modela.

Za to bi moral Urad za UI sodelovati z znanstveno skupnostjo, industrijo, civilno družbo in drugimi strokovnjaki. Pragovi ter orodja in merila za ocenjevanje zmogljivosti z visoko učinkovitostjo bi morali v veliki meri predvideti splošno naravo, zmogljivosti in povezano sistemsko tveganje modelov UI za splošne namene ter bi lahko upoštevali način dajanja modela na trg ali število uporabnikov, na katere bi lahko vplival. Za dopolnitev tega sistema bi morala Komisija imeti možnost, da sprejme posamezne odločitve, s katerimi model UI za splošne namene določi kot model UI za splošne namene s sistemskim tveganjem, če se ugotovi, da ima tak model zmogljivosti ali učinek, enakovreden tistim, zajetim z določenim pragom. To odločitev bi bilo treba sprejeti na podlagi splošne ocene meril za določitev modela UI za splošne namene s sistemskim tveganjem iz ene od prilog k tej uredbi, kot so kakovost ali velikost nabora učnih podatkov, število poslovnih in končnih uporabnikov, načini njihovega vnosa in izhoda, stopnja avtonomije in nadgradljivosti ali orodja, do katerih ima dostop. Komisija bi morala na obrazloženo zahtevo ponudnika, katerega model je bil označen za model UI za splošne namene s sistemskim tveganjem, upoštevati zahtevo in se lahko odloči, da ponovno oceni, ali lahko za model UI za splošne namene še vedno šteje, da predstavlja sistemska tveganja.

- (112) Pojasniti je treba tudi postopek za razvrstitev modela UI za splošne namene s sistemskimi tveganji. Za model UI za splošne namene, ki izpolnjuje veljavni prag za zmogljivosti z visoko učinkovitostjo, bi bilo treba domnevati, da je splošni model UI s sistemskim tveganjem. Ponudnik bi moral Urad za UI obvestiti najpozneje dva tedna po tem, ko so zahteve izpolnjene ali ko je znano, da bo model UI za splošne namene izpolnjeval zahteve, ki vodijo do te domneve. To je zlasti pomembno v zvezi s pragom operacij s plavajočo vejico, saj je pri učenju modelov UI za splošne namene potrebno precejšnje načrtovanje, ki vključuje vnaprejšnjo dodelitev računalniških virov, zato lahko ponudniki modelov UI za splošne namene vedo, ali bi njihov model dosegel prag pred zaključkom učenja. V okviru tega obvestila bi moral biti ponudnik sposoben dokazati, da model UI za splošne namene zaradi svojih posebnih značilnosti izjemoma ne predstavlja sistemskih tveganj in ga zato ne bi smeli razvrstiti kot model UI za splošne namene s sistemskimi tveganji. Te informacije so dragocene za Urad za UI pri predvidevanju dajanja modelov UI za splošne namene s sistemskimi tveganji na trg, ponudniki pa lahko začnejo zgodaj sodelovati z Uradom za UI. Te informacije so zlasti pomembne v zvezi z modeli UI za splošne namene, za katere se načrtuje, da bodo objavljeni kot odprtokodni, saj bo po objavi odprtokodnega modela morda težje izvajati potrebne ukrepe za zagotovitev skladnosti z obveznostmi iz te uredbe.

- (113) Če Komisija ugotovi, da model UI za splošne namene izpolnjuje zahteve za razvrstitev kot model UI za splošne namene s sistemskim tveganjem, ki pred tem ni bil znan ali o njem zadevni ponudnik ni obvestil Komisije, bi morala biti Komisija pooblaščenca, da ga tako označi. Sistem kvalificiranih opozoril bi moral zagotavljati, da znanstveni odbor obvešča Urad za UI o modelih UI za splošne namene, ki bi jih morebiti bilo treba razvrstiti kot modele UI za splošne namene s sistemskim tveganjem, ter da ima Urad pregled nad lastnimi dejavnostmi spremljanja.
- (114) Za ponudnike modelov UI za splošne namene s sistemskimi tveganji bi morale poleg obveznosti, ki veljajo za ponudnike modelov UI za splošne namene, veljati tudi obveznosti, namenjene prepoznavanju in zmanjšanju teh tveganj ter zagotavljanju ustrezne ravni kibernetske varnosti, ne glede na to, ali se zagotavljajo kot samostojni modeli ali so vgrajeni v sistem UI ali proizvod. Za doseganje teh ciljev bi morala ta uredba od ponudnikov zahtevati, da izvedejo potrebne ocene modelov, zlasti pred prvim dajanjem na trg, vključno z izvajanjem in dokumentiranjem testiranja modelov po načelu kontradiktornosti, po potrebi tudi z notranjim ali neodvisnim zunanjim testiranjem. Poleg tega bi morali ponudniki modelov UI za splošne namene s sistemskimi tveganji redno ocenjevati in zmanjševati sistemska tveganja, med drugim na primer z uvedbo politik za obvladovanje tveganj, kot so postopki za zagotavljanje odgovornosti in upravljanja, spremljanjem po dajanju na trg, sprejetjem ustreznih ukrepov v celotnem življenjskem ciklu modela in sodelovanjem z ustreznimi akterji v celotni verigi vrednosti UI.

- (115) Ponudniki modelov UI za splošne namene s sistemskimi tveganji bi morali oceniti in zmanjšati morebitna sistemska tveganja. Če razvoj ali uporaba modela kljub prizadevanjem za prepoznavanje in preprečevanje tveganj, povezanih z modelom UI za splošne namene, ki lahko predstavlja sistemska tveganja, povzroči resen incident, bi ga moral ponudnik modela UI za splošne namene brez nepotrebnega odlašanja spremljati ter Komisiji in pristojnim nacionalnim organom poročati o vseh ustreznih informacijah in možnih popravnihi ukrepih. Poleg tega bi morali ponudniki po potrebi zagotoviti ustrezno raven kibernetске varnosti modela in njegove fizične infrastrukture v celotnem življenjskem ciklu modela. Pri kibernetски varnosti zaradi sistemskih tveganj, povezanih z zlonamerno uporabo ali napadi, bi bilo treba ustrezno upoštevati naključno uhajanje iz modelov, nedovoljene različice, izogibanje varnostnim ukrepom in obrambo pred kibernetскими napadi, nepooblaščenim dostopom ali krajo modela. Tovrstno varnost bi bilo mogoče olajšati z zaščito uteži modelov, algoritmov, strežnikov in naborov podatkov, na primer z operativnimi varnostnimi ukrepi za informacijsko varnost, posebnimi politikami na področju kibernetске varnosti, ustreznimi tehničnimi in uveljavljenimi rešitvami ter kibernetским in fizičnim nadzorom dostopa, ki bi bili prilagojeni zadevnim okoliščinam in povezanim tveganjem.

- (116) Urad za UI bi moral spodbujati in olajšati pripravo, pregled in prilagoditev kodeksov prakse in pri tem upoštevati mednarodne pristope. K sodelovanju bi lahko bili povabljeni vsi ponudniki modelov UI za splošne namene. Za zagotovitev, da se v kodeksih prakse odražajo najsodobnejši tehnološki dosežki in ustrezno upoštevajo različni vidiki, bi moral Urad za UI pri pripravi teh kodeksov sodelovati z ustreznimi pristojnimi nacionalnimi organi, po potrebi pa bi se lahko posvetoval z organizacijami civilne družbe ter drugimi ustreznimi deležniki in strokovnjaki, vključno z znanstvenim odborom. V teh kodeksih prakse bi morale biti določene obveznosti za ponudnike modelov UI za splošne namene in modelov UI za splošne namene s sistemskimi tveganji. Kar zadeva sistemska tveganja, bi morali kodeksi prakse poleg tega prispevati k vzpostavitvi taksonomije tveganja za vrsto in naravo sistemskih tveganj na ravni Unije, vključno z njihovimi viri. Kodeksi prakse bi morali biti osredotočeni tudi na specifične ocene tveganja in ukrepe za zmanjšanje tveganj.

- (117) Kodeksi prakse bi morali biti osrednje orodje za pravilno izpolnjevanje obveznosti za ponudnike modelov UI za splošne namene, ki so določene v tej uredbi. Ponudniki bi morali imeti možnost, da se pri dokazovanju izpolnjevanja obveznosti oprejo na kodekse prakse. Komisija se lahko odloči, da z izvedbenimi akti odobri kodeks prakse in mu podeli splošno veljavnost v Uniji oziroma, kot nadomestno možnost, določi skupna pravila za izvajanje ustreznih obveznosti, če kodeksa prakse do začetka uporabe te uredbe ni mogoče dokončati ali če ga Urad za UI ne šteje za ustreznega. Ko je harmonizirani standard objavljen in ko ga Urad za UI oceni kot primerne za izpolnjevanje ustreznih obveznosti, bi morala za ponudnike veljati domneva o skladnosti, kadar ti izpolnjujejo evropski harmonizirani standard. Ponudniki modelov UI za splošne namene bi morali biti poleg tega sposobni z nadomestnimi ustreznimi sredstvi dokazati skladnost, če kodeksi prakse ali harmonizirani standardi niso na voljo ali če se odločijo, da se nanje ne bodo zanašali.

- (118) Ta uredba ureja sisteme UI in modele UI, saj za zadevne udeležence na trgu, ki te sisteme in modele dajejo na trg, v uporabo ali jih uporabljajo v Uniji, določa nekatere zahteve in obveznosti, s tem pa dopolnjuje obveznosti za ponudnike posredniških storitev, ki take sisteme ali modele vgrajujejo v svoje storitve, ki jih ureja Uredba (EU) 2022/2065. Kolikor so taki sistemi ali modeli vgrajeni v zelo velike spletne platforme ali zelo velike spletne iskalnike, zanje velja okvir za obvladovanje tveganj iz Uredbe (EU) 2022/2065. Zato bi bilo treba domnevati, da so ustrezne obveznosti iz te uredbe izpolnjene, razen če se v takih modelih pojavijo in prepoznajo pomembna sistemska tveganja, ki niso zajeta v Uredbi (EU) 2022/2065. V tem okviru morajo ponudniki zelo velikih spletnih platform in zelo velikih spletnih iskalnikov oceniti morebitna sistemska tveganja, ki izhajajo iz zasnove, delovanja in uporabe njihovih storitev, vključno s tem, kako zasnova algoritemskih sistemov, ki se uporabljajo v storitvi, lahko prispeva k takim tveganjem, pa tudi sistemska tveganja, ki izhajajo iz morebitne napačne uporabe. Ti ponudniki morajo ob spoštovanju temeljnih pravic sprejeti tudi ustrezne ukrepe za zmanjšanje tveganj.

- (119) Glede na hiter tempo inovacij in tehnološkega razvoja digitalnih storitev, ki spadajo na področje uporabe različnih instrumentov prava Unije, zlasti glede na uporabo in dožemanje oseb, ki so jim namenjeni, se lahko sistemi UI, za katere se uporablja ta uredba, zagotavljajo kot posredniške storitve ali kot deli posredniških storitev v smislu Uredbe (EU) 2022/2065, ki bi jo bilo treba razlagati na tehnološko nevtralen način. Sistemi UI se lahko na primer uporabljajo za zagotavljanje spletnih iskalnikov, zlasti če sistem UI, kot je spletni klepetalni robot, načeloma izvaja poizvedbe na vseh spletiščih, nato pa rezultate vključi v svoje obstoječe znanje in posodobljeno znanje uporabi za ustvarjanje enega samega izhodnega podatka, v katerem so združeni različni viri informacij.
- (120) Poleg tega so obveznosti za ponudnike in uvajalce nekaterih sistemov UI iz te uredbe, ki omogočajo odkrivanje in razkrivanje dejstva, da so izhodni podatki teh sistemov umetno ustvarjeni ali prirejeni, še zlasti pomembne zato, da se olajša učinkovito izvajanje Uredbe (EU) 2022/2065. To velja zlasti za obveznosti za ponudnike zelo velikih spletnih platform ali zelo velikih spletnih iskalnikov, da prepoznajo in zmanjšajo sistemska tveganja, ki lahko izhajajo iz razširjanja umetno ustvarjenih ali prirejenih vsebin, zlasti tveganje dejanskih ali predvidljivih negativnih učinkov na demokratične procese, državljansko razpravo in volilne procese, tudi z dezinformacijami.

- (121) Standardizacija bi morala imeti ključno vlogo pri zagotavljanju tehničnih rešitev ponudnikom, da se zagotovi skladnost s to uredbo, ob upoštevanju najsodobnejših tehnoloških dosežkov, ter pri spodbujanju inovacij, konkurenčnosti in rasti na enotnem trgu. Skladnost s harmoniziranimi standardi, kot so opredeljeni v členu 2, točka 1(c), Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta⁴¹ in od katerih se običajno pričakuje, da odražajo najsodobnejše tehnološke dosežke, bi morala predstavljati sredstvo, s katerim ponudniki dokažejo skladnost z zahtevami iz te uredbe. Zato bi bilo treba spodbujati uravnoteženo zastopanost interesov z vključitvijo vseh ustreznih deležnikov v razvoj standardov, zlasti MSP, potrošniških organizacij ter okoljskih in socialnih deležnikov v skladu s členoma 5 in 6 Uredbe (EU) št. 1025/2012. Da bi lažje dosegli skladnost, bi morala Komisija brez nepotrebne odlašanja izdati zahteve za standardizacijo. Pri pripravi zahteve za standardizacijo se Komisija posvetuje s svetovalnim forumom in Odborom, da zbere ustrezno strokovno znanje. Ker pa ustrezni sklici na harmonizirane standarde še ne obstajajo, bi morala imeti Komisija možnost, da z izvedbenimi akti in po posvetovanju s svetovalnim forumom določi skupne specifikacije za nekatere zahteve iz te uredbe.

⁴¹ Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12).

Skupna specifikacija bi morala biti izjemna nadomestna rešitev, da se ponudniku olajša izpolnjevanje obveznosti glede skladnosti z zahtevami iz te uredbe, kadar nobena od evropskih organizacij za standardizacijo ne sprejme zahteve za standardizacijo ali kadar ustrezni harmonizirani standardi nezadostno obravnavajo pomisleke glede temeljnih pravic ali kadar harmonizirani standardi niso skladni z zahtevo ali kadar pride do zamud pri sprejetju ustreznega harmoniziranega standarda. Kadar je vzrok za takšno zamudo pri sprejetju harmoniziranega standarda tehnična kompleksnost zadevnega standarda, bi morala Komisija to upoštevati preden se odloči za določitev skupnih specifikacij. Komisija naj pri pripravi skupnih specifikacij sodeluje z mednarodnimi partnerji in mednarodnimi organi za standardizacijo.

- (122) Brez poseganja v uporabo harmoniziranih standardov in skupnih specifikacij je primerno, da se za ponudnike visokotvegane sistema UI, ki je bil naučen in testiran na podlagi podatkov, ki odražajo specifično geografsko, vedenjsko, vsebinsko ali funkcionalno okolje, v katerem naj bi se ta sistem uporabljal, domneva, da delujejo skladno z ustreznim ukrepom, določenim na podlagi zahteve glede upravljanja podatkov iz te uredbe. Brez poseganja v zahteve glede robustnosti in točnosti iz te uredbe bi bilo treba v skladu s členom 54(3) Uredbe (EU) 2019/881 domnevati, da so visokotvegani sistemi UI, ki so bili certificirani ali za katere je bila izdana izjava o skladnosti v okviru sheme za kibernetško varnost na podlagi navedene uredbe, ob tem pa so bili sklici na zadevno shemo objavljeni v *Uradnem listu Evropske unije*, skladni z zahtevo glede kibernetške varnosti iz te uredbe, če certifikat kibernetške varnosti ali izjava o skladnosti ali njen del vključuje zahtevo glede kibernetške varnosti iz te uredbe. To ne posega v prostovoljno naravo navedene sheme za kibernetško varnost.
- (123) Da bi zagotovili visoko raven zaupanja v visokotvegane sisteme UI, bi bilo treba za te sisteme pred dajanjem na trg ali v uporabo opraviti ugotavljanje skladnosti.

- (124) Da bi čim bolj zmanjšali breme za operaterje in se izognili morebitnemu podvajanju, je primerno, da bi skladnost visokotveganih sistemov UI, povezanih s proizvodi, za katere velja obstoječa harmonizacijska zakonodaja Unije, ki temelji na novem zakonodajnem okviru, z zahtevami te uredbe ocenili v okviru ugotavljanja skladnosti, kot je že določeno navedena zakonodaja. Uporaba zahtev iz te uredbe torej ne bi smela vplivati na posebno logiko, metodologijo ali splošno strukturo ugotavljanja skladnosti na podlagi ustrezne harmonizacijske zakonodaje Unije.
- (125) Zaradi kompleksnosti visokotveganih sistemov UI in z njimi povezanih tveganj je pomembno razviti ustrezen postopek ugotavljanja skladnosti visokotveganih sistemov UI, ki vključuje priglašene organe, tako imenovano ugotavljanje skladnosti s strani tretjih oseb. Glede na sedanje izkušnje poklicnih izdajateljev potrdil pred dajanjem na trg na področju varnosti proizvodov in glede na različno naravo zadevnih tveganj, pa je primerno, da se vsaj v začetni fazi uporabe te uredbe omeji področje uporabe ugotavljanja skladnosti s strani tretjih oseb na visokotvegane sisteme UI, ki niso povezani s proizvodi. Zato bi moral ugotavljanje skladnosti takih sistemov praviloma opraviti ponudnik na lastno odgovornost, z edino izjemo sistemov UI, namenjenih uporabi za biometriko.

- (126) Za izvedbo ugotavljanja skladnosti s strani tretjih oseb, kadar je potrebno, bi morali pristojni nacionalni organi na podlagi te uredbe prigrasiti prigrasene organe, pod pogojem, da izpolnjujejo vrsto zahtev, zlasti glede neodvisnosti, kompetenc, neobstoja navzkrižja interesov, pa tudi zahtev glede kibernetiske varnosti. Pristojni nacionalni organi bi morali prigrasitev teh organov poslati Komisiji in drugim državam članicam prek elektronskega orodja za prigrasitev, ki ga razvije in upravlja Komisija na podlagi člena R23 Priloge I k Sklepu št. 768/2008/ES.
- (127) V skladu z zavezami Unije iz Sporazuma Svetovne trgovinske organizacije o tehničnih ovirah v trgovini je ustrezno olajšati vzajemno priznavanje rezultatov ugotavljanja skladnosti, ki jih pridobijo pristojni organi za ugotavljanje skladnosti ne glede na to, kje imajo sedež, pod pogojem, da navedeni organi za ugotavljanje skladnosti, ustanovljeni na podlagi prava tretje države, izpolnjujejo veljavne zahteve iz te uredbe in če je Unija v ta namen sklenila sporazum. V zvezi s tem bi morala Komisija v ta namen dejavno preučiti morebitne mednarodne instrumente in si zlasti prizadevati za sklenitev sporazumov s tretjimi državami o vzajemnem priznavanju.

- (128) V skladu s skupno uveljavljenim pojmom bistvene spremembe za proizvode, ki jih ureja harmonizacijska zakonodaja Unije, je primerno, da ob vsaki spremembi, ki bi lahko vplivala na skladnost visokotveganega sistema UI s to uredbo (npr. spremembi arhitekture operacijskega sistema ali programske opreme), ali kadar se spremeni predvideni namen sistema, ta sistem UI šteje za nov sistem UI, za katerega bi bilo treba opraviti novo ugotavljanje skladnosti. Vendar spremembe algoritma in zmogljivosti sistemov UI, ki se po tem, ko so dani na trg ali v uporabo, še naprej „učijo“, tj. samodejno prilagajajo način izvajanja funkcij, ne bi smele pomeniti bistvene spremembe, če jih je ponudnik določil vnaprej in ocenil v okviru ugotavljanja skladnosti.
- (129) Visokotvegani sistemi UI bi morali imeti oznako CE, ki označuje njihovo skladnost s to uredbo, da se lahko prosto gibljejo na notranjem trgu. Visokotvegani sistemi UI, ki so vgrajeni v proizvod, bi morali biti označeni s fizično oznako CE, ki jo lahko dopolnjuje digitalna oznaka CE. Za visokotvegane sisteme UI, ki se zagotavljajo samo digitalno, bi bilo treba uporabljati digitalno oznako CE. Države članice ne bi smele neupravičeno ovirati dajanja na trg ali v uporabo visokotveganih sistemov UI, ki izpolnjujejo zahteve iz te uredbe in nosijo oznako CE.

- (130) V določenih okoliščinah je lahko hitra razpoložljivost inovativnih tehnologij ključnega pomena za zdravje in varnost ljudi, varstvo okolja in podnebne spremembe ter za družbo kot celoto. Zato je primerno, da bi iz izjemnih razlogov javne varnosti ali varstva življenja in zdravja fizičnih oseb, varstva okolja ter zaščite ključne industrijskih in infrastrukturnih sredstev organi za nadzor trga lahko dovolili dajanje na trg ali v uporabo sistemov UI, za katere ugotavljanje skladnosti ni bilo opravljeno. V ustrezno utemeljenih primerih, kot je določeno v tej uredbi, lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali organi civilne zaščite dajo določen visokotvegani sistem UI v uporabo brez dovoljenja organa za nadzor trga, če se za tako dovoljenje brez nepotrebnega odlašanja zaprosi med uporabo ali po njej.
- (131) Da bi olajšali delo Komisije in držav članic na področju UI ter povečanje preglednosti za javnost, bi bilo treba od ponudnikov visokotveganih sistemov UI, razen tistih, povezanih s proizvodi, ki spadajo na področje uporabe ustrezne obstoječe harmonizacijske zakonodaje Unije, ter ponudnikov, ki menijo, da sistem UI s seznama visokotveganih primerov uporabe iz priloge k tej uredbi, ni visokotvegani na podlagi odstopanja, zahtevati, da se registrirajo v podatkovni zbirki EU, ki jo vzpostavi in upravlja Komisija, in da v tej zbirki beležijo tudi informacije o svojih sistemih UI. Pred uporabo sistema UI s seznama visokotveganih primerov uporabe iz priloge k tej uredbi bi se morali uvajalci visokotveganih sistemov UI, ki so javni organi, agencije ali telesa, registrirati v taki zbirki in izbrati sistem, ki ga nameravajo uporabljati.

Drugi uvajalci bi morali imeti pravico do prostovoljne registracije. Ta del podatkovne zbirke EU bi moral biti javno dostopen in brezplačen, informacije pa bi morale biti zlahka dostopne, razumljive in strojno berljive. Podatkovna zbirka EU bi prav tako morala biti prilagojena uporabnikom, na primer z zagotavljanjem funkcije iskanja, tudi s ključnimi besedami, da bi širša javnost lahko našla ustrezne informacije, ki se predložijo ob registraciji visokotveganih sistemov UI in o primeru uporabe visokotveganih sistemov UI iz priloge k tej uredbi za zadevne visokotvegane sisteme UI. V podatkovni zbirki EU bi bilo treba registrirati tudi bistvene spremembe visokotveganih sistemov UI. Za visokotvegane sisteme UI na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja bi bilo treba obveznosti registracije izpolniti v varnem, nejavnem delu podatkovne zbirke EU. Dostop do varnega dela, ki ni dostopen javnosti, bi moral biti strogo omejen na Komisijo in organe za nadzor trga, kar zadeva njihov nacionalni del te podatkovne zbirke. Visokotvegani sistemi UI na področju kritične infrastrukture bi morali biti registrirani le na nacionalni ravni. Komisija bi morala biti upravljevec podatkovne zbirke EU v skladu z Uredbo (EU) 2018/1725. Za zagotovitev polne funkcionalnosti podatkovne zbirke ob njeni uvedbi bi moral postopek za njeno vzpostavitev vključevati razvoj funkcionalnih specifikacij s strani Komisije in neodvisno revizijsko poročilo. Komisija bi morala pri opravljanju nalog upravljavca podatkov v podatkovni zbirki EU upoštevati tveganja, povezana s kibernetско varnostjo. Podatkovna zbirka EU, vključno z informacijami, ki so prek nje na voljo, bi morala izpolnjevati zahteve iz Direktive (EU) 2019/882, da bi bila javnosti čim bolj dostopna in uporabna.

- (132) Nekateri sistemi UI, namenjeni stikom s fizičnimi osebami ali ustvarjanju vsebine, lahko predstavljajo posebna tveganja izdajanja za drugo osebo ali zavajanja, ne glede na to, ali se uvrščajo med sisteme visokega tveganja ali ne. V določenih okoliščinah bi zato za uporabo teh sistemov morale veljati posebne obveznosti glede preglednosti, brez poseganja v zahteve in obveznosti za visokotvegane sisteme UI, in ciljne izjeme, da bi upoštevali posebne potrebe na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Zlasti bi bilo treba fizične osebe obvestiti, da so v interakciji s sistemom UI, razen če je to očitno z vidika fizične osebe, ki je razmeroma dobro obveščena, pozorna in preudarna, ob upoštevanju okoliščin in okvira uporabe. Pri izvajanju te obveznosti bi bilo treba upoštevati značilnosti fizičnih oseb, ki zaradi svoje starosti ali invalidnosti pripadajo ranljivim skupinam, kolikor je namen sistema UI tudi interakcija s temi skupinami. Poleg tega bi bilo treba fizične osebe obvestiti, kadar so izpostavljene sistemom UI, ki lahko z obdelavo njihovih biometričnih podatkov prepoznajo čustva ali namere teh oseb ali sklepajo o njih oziroma te osebe razvrstijo v posebne kategorije. Tovrstne posebne kategorije se lahko nanašajo na značilnosti, kot so spol, starost, barva las, barva oči, tetovaže, osebne lastnosti, etnično poreklo, osebne želje in interesi. Take informacije in obvestila bi bilo treba zagotoviti v invalidom dostopnih oblikah.

- (133) Različni sistemi UI lahko ustvarijo velike količine sintetičnih vsebin, ki jih ljudje vse težje razlikujejo od vsebin, ki jih ustvari človek, in verodostojnih vsebin. Široka razpoložljivost in večje zmogljivosti teh sistemov pomembno vplivajo na integriteto informacijskega ekosistema in zaupanje vanj, saj se pojavljajo nova tveganja dezinformacij in obsežnega prirejanja, goljufij, izdajanja za drugo osebo in zavajanja potrošnikov. Glede na navedene vplive, hiter tempo tehnološkega razvoja ter potrebo po novih metodah in tehnikah za sledenje izvoru informacij je primerno od ponudnikov navedenih sistemov zahtevati, da vključijo tehnične rešitve, ki v strojno berljivi obliki omogočajo označevanje in zaznavanje, da je izhodne podatke ustvaril ali priredil sistem UI in ne človek. Take tehnike in metode bi morale biti dovolj zanesljive, interoperabilne, učinkovite in robustne, kolikor je to tehnično izvedljivo, ob upoštevanju razpoložljivih tehnik ali kombinacije takih tehnik, kot so vodni žigi, prepoznavanje metapodatkov, kriptografske metode za dokazovanje izvora in pristnosti vsebine, metode beleženja, prstni odtisi ali druge tehnike, kot je ustrezno. Ponudniki bi morali pri izvajanju te obveznosti upoštevati tudi posebnosti in omejitve različnih vrst vsebin ter zadevni tehnološki in tržni razvoj na tem področju, pokazatelj katerega so splošno priznani najsodobnejši tehnološki dosežki. Takšne tehnike in metode se lahko izvajajo na ravni sistema UI ali na ravni modela UI, vključno z modeli UI za splošne namene, ki ustvarjajo vsebino, da se ponudniku sistema UI nižje v verigi omogoči lažje izpolnjevanje te obveznosti. Da bi ta obveznost označevanja ostala sorazmerna, je primerno predvideti, da ne bi smela zajemati sistemov UI, ki zagotavljajo predvsem podporno funkcijo za standardno urejanje, ali sistemov UI, ki ne spreminjajo bistveno vhodnih podatkov, ki jih zagotovi uvajalec, ali njihove semantike.

- (134) Poleg tehničnih rešitev, ki jih uporabljajo ponudniki sistema UI, bi morali uvajalci, ki sistem UI uporabljajo za ustvarjanje ali prirejanje slikovnih, zvočnih ali video vsebin, ki v znatni meri spominjajo na obstoječe osebe, predmete, mesta ali dogodke in bi se osebi zmotno zdele verodostojne ali resnične (globoki ponaredki), na jasen in razpoznaven način tudi razkriti, da je bila vsebina umetno ustvarjena ali prirejena, tako da ustrezno označijo izhodne podatke UI in razkrijejo njihov umetni izvor. Skladnost s to obveznostjo glede preglednosti se ne bi smela razlagati tako, da pomeni, da uporaba sistema UI ali njegovih izhodnih podatkov ovira pravico do svobode izražanja ter pravico do svobode umetnosti in znanosti, ki ju zagotavlja Listina, zlasti kadar je vsebina del očitno ustvarjalnega, satiričnega, umetniškega, izmišljenega ali podobnega dela ali programa, ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb. V teh primerih je obveznost glede preglednosti za globoke ponaredke iz te uredbe omejena na to, da se obstoj tako ustvarjenih ali prirejenih vsebin ustrezno razkrije na način, ki ne ovira prikazovanja dela ali uživanja v njem, vključno z njegovo običajno eksploatacijo in uporabo, ob ohranjanju uporabnosti in kakovosti dela. Primerno je tudi predvideti podobno obveznost razkritja v zvezi z besedilom, ustvarjenim ali prirejenim z UI, če je objavljeno z namenom obveščanja javnosti o zadevah javnega interesa, razen če je vsebino, ustvarjeno z UI, pregledal človek ali urednik, ob tem pa fizična ali pravna oseba nosi uredniško odgovornost za objavo vsebine.

- (135) Komisija lahko brez poseganja v obvezno naravo in polno uporabo obveznosti glede preglednosti prav tako spodbuja in olajšuje pripravo kodeksov prakse na ravni Unije, da se olajša učinkovito izvajanje obveznosti v zvezi z odkrivanjem in označevanjem umetno ustvarjenih ali prirejenih vsebin, po potrebi vključno s podporo praktičnim ureditvam za omogočanje dostopa do mehanizmov odkrivanja, in olajšanje sodelovanja z drugimi akterji vzdolž verige vrednosti, razširjanje vsebine ali preverjanje njene pristnosti in izvora, da se javnosti omogoči učinkovito razlikovanje vsebin, ustvarjenih z UI.
- (136) Obveznosti za ponudnike in uvajalce nekaterih sistemov UI iz te uredbe, da omogočijo odkrivanje in razkrivanje dejstva, da so izhodni podatki teh sistemov umetno ustvarjeni ali prirejeni, so še zlasti pomembne, da se olajša učinkovito izvajanje Uredbe (EU) 2022/2065. To velja zlasti za obveznosti za ponudnike zelo velikih spletnih platform ali zelo velikih spletnih iskalnikov, da prepoznajo in zmanjšajo sistemska tveganja, ki lahko izhajajo iz razširjanja umetno ustvarjenih ali prirejenih vsebin, zlasti tveganje dejanskih ali predvidljivih negativnih učinkov na demokratične procese, državljansko razpravo in volilne procese, tudi z dezinformacijami. Zahteva za označevanje s sistemi UI ustvarjenih vsebin na podlagi te uredbe ne posega v obveznost iz člena 16(6) Uredbe (EU) 2022/2065, da ponudniki storitev gostovanja obravnavajo prijave nezakonitih vsebin, prejete na podlagi člena 16(1) navedene uredbe, ter ne bi smela vplivati na oceno in odločitev o nezakonitosti določene vsebine. To oceno bi bilo treba opraviti izključno ob upoštevanju pravil, ki urejajo zakonitost vsebine.

- (137) Skladnosti z navedenimi obveznostmi glede preglednosti za sisteme UI iz te uredbe ne bi smeli razlagati tako, da pomeni, da je uporaba sistema UI ali njegovih izhodnih podatkov zakonita na podlagi te uredbe ali drugega prava Unije in prava držav članic, ter ne bi smela posegati v druge obveznosti uvajalcev sistemov UI glede preglednosti, določene v pravu Unije ali nacionalnem pravu.
- (138) UI je hitro razvijajoča se skupina tehnologij, ki zahteva regulativni nadzor ter varen in nadzorovan prostor za eksperimentiranje, ob zagotavljanju odgovornih inovacij ter vključevanja ustreznih zaščitnih ukrepov in ukrepov za zmanjšanje tveganj. Da bi zagotovili pravni okvir, ki spodbuja inovacije ter je primeren za prihodnost in odporen na motnje, bi morale države članice zagotoviti, da njihovi nacionalni pristojni organi na nacionalni ravni vzpostavijo vsaj en regulativni peskovnik za UI, da bi olajšali razvoj in testiranje inovativnih sistemov UI pod strogim regulativnim nadzorom, preden se ti sistemi dajo na trg ali kako drugače v uporabo. Države članice bi lahko to obveznost izpolnile tudi s sodelovanjem v že obstoječih regulativnih peskovnikih ali z vzpostavitvijo peskovnika skupaj s pristojnimi organi ene ali več držav članic, če tako sodelovanje sodelujočim državam članicam zagotavlja enakovredno raven nacionalne pokritosti. Regulativni peskovniki za UI bi lahko bili vzpostavljeni v fizični, digitalni ali hibridni obliki ter za fizične in digitalne izdelke. Organi, ki vzpostavijo regulativne peskovnike za UI, bi morali tudi zagotoviti, da imajo ti peskovniki ustrezne vire za svoje delovanje, vključno s finančnimi in človeškimi viri.

- (139) Cilji regulativnih peskovnikov za UI bi morali biti spodbujanje inovacij na področju UI z vzpostavitev nadzorovanega okolja za eksperimentiranje in testiranje v fazi razvoja ter pred trženjem, da se zagotovi skladnost inovativnih sistemov UI s to uredbo ter drugim ustreznim pravom Unije in nacionalnim pravom. Poleg tega bi moral biti cilj regulativnih peskovnikov za UI okrepitev pravne varnosti za inovatorje ter nadzora pristojnih organov in njihovega razumevanja priložnosti, nastajajočih tveganj in vplivov uporabe UI, olajšanje regulativnega učenja za organe in podjetja, tudi zaradi prihodnjih prilagoditev pravnega okvira, podpiranje sodelovanja in izmenjave najboljših praks z organi, vključenimi v regulativni peskovnik za UI, pa tudi pospešitev dostopa do trgov, med drugim z odpravo ovir za MSP, vključno z zagonskimi podjetji. Regulativni peskovniki za UI bi morali biti široko dostopni po vsej Uniji, posebno pozornost pa bi bilo treba nameniti njihovi dostopnosti za MSP, vključno z zagonskimi podjetji. Sodelovanje v regulativnem peskovniku za UI bi moralo biti osredotočeno na vprašanja, ki ustvarjajo pravno negotovost za ponudnike in potencialne ponudnike pri inovacijah, eksperimentiranju z UI v Uniji in prispevanju k regulativnemu učenju, ki temelji na dokazih. Nadzor sistemov UI v regulativnem peskovniku za UI bi zato moral zajemati njihov razvoj, učenje, testiranje in validacijo, preden so sistemi dani na trg ali v uporabo, ter pojem in pojav bistvenih sprememb, zaradi katerih bi lahko bil potreben nov postopek ugotavljanja skladnosti. Vsa pomembna tveganja, prepoznana med razvojem in testiranjem takih sistemov UI, bi bilo treba ustrezno zmanjšati, če to ni mogoče, pa postopek razvoja in testiranja ustaviti.

Kadar je primerno, bi morali pristojni nacionalni organi, ki vzpostavijo regulativne peskovnike za UI, sodelovati z drugimi ustreznimi organi, vključno s tistimi, ki nadzirajo varstvo temeljnih pravic, in bi lahko omogočili sodelovanje drugih akterjev v ekosistemu UI, kot so nacionalne ali evropske organizacije za standardizacijo, priglašeni organi, centri za testiranje in eksperimentiranje, laboratoriji za raziskave in eksperimentiranje, evropska vozlišča za digitalne inovacije ter ustrezne organizacije deležnikov in civilne družbe. Za zagotovitev enotnega izvajanja po vsej Uniji in ekonomije obsega je primerno določiti skupna pravila za izvajanje regulativnih peskovnikov za UI in okvir za sodelovanje med ustreznimi organi, vključenimi v nadzor peskovnikov. Regulativni peskovniki za UI, vzpostavljeni na podlagi te uredbe, ne bi smeli posegati v drugo pravo, ki omogoča vzpostavitev drugih peskovnikov, katerih namen je zagotoviti skladnost s pravom, ki ni ta uredba. Ustrezni pristojni organi, odgovorni za te druge regulativne peskovnike, bi morali, kadar je primerno, upoštevati koristi uporabe teh peskovnikov tudi za namen zagotavljanja skladnosti sistemov UI s to uredbo. Po dogovoru med pristojnimi nacionalnimi organi in udeleženci v regulativnem peskovniku za UI se lahko testiranje v realnih razmerah izvaja in nadzira tudi v okviru regulativnega peskovnika za UI.

- (140) Ta uredba bi morala zagotoviti pravno podlago, da ponudniki in potencialni ponudniki v regulativnem peskovniku za UI osebne podatke, zbrane za druge namene, uporabijo za razvoj nekaterih sistemov UI v javnem interesu v okviru regulativnega peskovnika za UI samo pod določenimi pogoji v skladu s členom 6(4) in členom 9(2), točka (g), Uredbe (EU) 2016/679, členi 5, 6 in 10 Uredbe (EU) 2018/1725 ter brez poseganja v člen 4(2) in člen 10 Direktive (EU) 2016/680. Vse druge obveznosti upravljavcev podatkov in pravice posameznikov, na katere se nanašajo osebni podatki, na podlagi uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktive (EU) 2016/680 se še naprej uporabljajo. Ta uredba zlasti ne bi smela zagotavljati pravne podlage v smislu člena 22(2), točka (b), Uredbe (EU) 2016/679 in člena 24(2), točka (b), Uredbe (EU) 2018/1725. Ponudniki in potencialni ponudniki v regulativnem peskovniku za UI bi morali zagotoviti ustrezne zaščitne ukrepe in sodelovati s pristojnimi organi, tudi z upoštevanjem njihovih smernic ter hitrim in dobronamernim ukrepanjem, da bi ustrezno zmanjšali vsa prepoznana znatna tveganja za varnost, zdravje in temeljne pravice, ki se lahko pojavijo med razvojem, testiranjem in eksperimentiranjem v tem peskovniku.

- (141) Da bi pospešili proces razvoja visokotveganih sistemov UI s seznama v eni od prilog k tej uredbi in njihovega dajanja na trg, je pomembno, da imajo tudi ponudniki ali potencialni ponudniki takih sistemov koristi od posebne ureditve za testiranje teh sistemov v realnih razmerah brez sodelovanja v regulativnem peskovniku za UI. Vendar bi bilo treba v takih primerih, ob upoštevanju možnih posledic takega testiranja za posameznike zagotoviti, da se s to uredbo za ponudnike ali potencialne ponudnike uvedejo ustrezna in zadostna jamstva in pogoji. Taka jamstva bi morala med drugim vključevati zahtevo, da je za sodelovanje fizičnih oseb pri testiranju v realnih razmerah potrebna informirana privolitev, razen ko gre za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ko bi pridobitev informirane privolitve preprečila testiranje sistema UI. Privolitev posameznikov, da sodelujejo pri takem testiranju na podlagi te uredbe, se razlikuje od privolitve posameznikov, na katere se nanašajo osebni podatki, v obdelavo njihovih osebnih podatkov na podlagi ustrezne zakonodaje o varstvu podatkov in vanjo ne posega.

Pomembno je tudi čim bolj zmanjšati tveganja in pristojnim organom omogočiti nadzor ter zato od potencialnih ponudnikov zahtevati, da imajo načrt testiranja v dejanskih razmerah, ki ga predložijo pristojnemu organu za nadzor trga, da testiranje registrirajo v namenskih delih podatkovne zbirke EU, ob upoštevanju nekaterih omejenih izjem, da določijo omejitve obdobja, v katerem je mogoče opraviti testiranje, in da zahtevajo dodatne zaščitne ukrepe za osebe, ki pripadajo določenim ranljivim skupinami, ter da imajo pisni dogovor, v katerem so opredeljene vloge in odgovornosti potencialnih ponudnikov in uvajalcev, ter učinkovit nadzor, ki ga izvaja usposobljeno osebje, vključeno v testiranje v realnih razmerah. Poleg tega je primerno predvideti dodatne zaščitne ukrepe za zagotovitev, da se lahko napovedi, priporočila ali odločitve sistema UI učinkovito izniči in zanemarijo ter da so osebni podatki zaščiteni in izbrisani, ko posamezniki umaknejo privolitev za sodelovanje v testiranju, brez poseganja v njihove pravice, ki jih imajo kot posamezniki, na katere se nanašajo osebni podatki, na podlagi prava Unije o varstvu podatkov. Kar zadeva prenos podatkov, je primerno predvideti tudi, da bi bilo treba podatke, zbrane in obdelane za namene testiranja v realnih razmerah, prenesti v tretje države le, če se izvajajo ustrezni in veljavni zaščitni ukrepi na podlagi prava Unije, zlasti v skladu z osnovami za prenos osebnih podatkov na podlagi prava Unije o varstvu podatkov, medtem ko so za neosebne podatke ustrezni zaščitni ukrepi vzpostavljeni v skladu s pravom Unije, kot sta uredbi (EU) 2022/868⁴² in (EU) 2023/2854⁴³ Evropskega parlamenta in Sveta.

⁴² Uredba (EU) 2022/868 Evropskega parlamenta in Sveta z dne 30. maja 2022 o evropskem upravljanju podatkov in spremembi Uredbe (EU) 2018/1724 (Akt o upravljanju podatkov) (UL L 152, 3.6.2022, str. 1).

⁴³ Uredba (EU) 2023/2854 Evropskega parlamenta in Sveta z dne 13. decembra 2023 o harmoniziranih pravilih za pravičen dostop do podatkov in njihovo uporabo ter spremembi Uredbe (EU) 2017/2394 in Direktive (EU) 2020/1828 (akt o podatkih) (UL L, 2023/2854, 22.12.2023, ELI: <http://data.europa.eu/eli/reg/2023/2854/oj>).

- (142) Da bi zagotovili, da bo UI privedla do družbeno in okoljsko koristnih rezultatov, se države članice spodbuja, naj podpirajo in spodbujajo raziskave in razvoj rešitev UI v podporo družbeno in okoljsko koristnim rezultatom, kot so rešitve, ki temeljijo na umetni inteligenci, za povečanje dostopnosti za invalide, odpravo socialno-ekonomskih neenakosti ali doseganje okoljskih ciljev, in sicer z dodelitvijo zadostnih sredstev, vključno z javnimi sredstvi in financiranjem Unije, ter, kadar je ustrezno in pod pogojem, da so izpolnjena merila za upravičenost in izbor, zlasti upoštevajoč projekte, ki vključujejo takšne cilje. Takšni projekti bi morali temeljiti na načelu interdisciplinarnega sodelovanja med razvijalci UI, strokovnjaki za neenakost in nediskriminacijo, dostopnost, potrošnike, okolje in digitalne pravice ter akademskimi krogi.

- (143) Za spodbujanje in zaščito inovacij je pomembno, da se upoštevajo interesi MSP, vključno z zagonskimi podjetji, ki so ponudniki ali uvajalci sistemov UI. V ta namen bi morale države članice razviti pobude, namenjene tem operaterjem, vključno z ozaveščanjem in sporočanjem informacij. Države članice bi morale MSP, vključno z zagonskimi podjetji, ki imajo registrirani sedež ali podružnico v Uniji, zagotoviti prednostni dostop do regulativnih peskovnikov za UI, če ti izpolnjujejo pogoje za upravičenost in merila za izbor, ter drugim ponudnikom in potencialnim ponudnikom ne preprečujejo dostopa do peskovnikov, če so izpolnjeni enaki pogoji in merila. Države članice bi morale uporabljati obstoječe kanale in po potrebi vzpostaviti nove namenske kanale za komunikacijo z MSP, vključno z zagonskimi podjetji, uvajalci, drugimi inovatorji in po potrebi z lokalnimi javnimi organi, da se MSP z zagotavljanjem smernic in odgovarjanjem na vprašanja o izvajanju te uredbe zagotovi podpora v celotnem razvojnem procesu. Ti kanali bi morali po potrebi sodelovati, da bi ustvarili sinergije in zagotovili homogenost svojih smernic za MSP, vključno z zagonskimi podjetji, in uvajalce. Države članice bi poleg tega morale olajševati sodelovanje MSP in drugih ustreznih deležnikov v postopkih razvoja standardizacije. Poleg tega bi se pri določanju pristojbin s strani priglašanih organov za ugotavljanje skladnosti morali upoštevati posebni interesi in potrebe ponudnikov, ki so MSP, vključno z zagonskimi podjetji. Komisija bi morala stroške certificiranja in skladnosti za MSP, vključno z zagonskimi podjetji, redno ocenjevati, in sicer s preglednimi posvetovanji, ter sodelovati z državami članicami za znižanje teh stroškov.

Na primer, stroški prevajanja, povezani z obvezno dokumentacijo in komuniciranjem z organi, lahko predstavljajo znaten strošek za ponudnike in druge operaterje, zlasti tiste manjšega obsega. Države članice bi morale po možnosti zagotoviti, da je eden od jezikov, ki jih določijo in sprejmejo za dokumentacijo zadevnih ponudnikov in za komunikacijo z operaterji, jezik, ki ga na splošno razume največje možno število čezmejnih uvajalcev. Za obravnavanje posebnih potreb MSP, vključno z zagonskimi podjetji, bi morala Komisija na zahtevo Odbora zagotoviti standardizirane predloge za področja, zajeta v tej uredbi. Poleg tega bi morala Komisija dopolniti prizadevanja držav članic z zagotovitvijo enotne informacijske platforme, ki vsebuje enostavno uporabne informacije v zvezi s to uredbo za vse ponudnike in uvajalce, organiziranjem ustreznih komunikacijskih kampanj za ozaveščanje o obveznostih, ki izhajajo iz te uredbe, ter ocenjevanjem in spodbujanjem zbliževanja najboljših praks v postopkih javnega naročanja v zvezi s sistemi UI. Srednja podjetja, ki so bila do nedavno opredeljena kot mala podjetja v smislu Priloge k Priporočilu Komisije 2003/361/ES⁴⁴, bi morala imeti dostop do teh podpornih ukrepov, saj ta nova srednja podjetja včasih morda nimajo pravnih sredstev in niso pridobila ustreznih usposabljanj, potrebnih za zagotovitev ustreznega razumevanja te uredbe in skladnosti z njo.

⁴⁴ Priporočilo Komisije z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

- (144) Za spodbujanje in zaščito inovacij bi morali platforma za UI na zahtevo, vsi ustrezni programi in projekti Unije za financiranje, kot sta programa Digitalna Evropa in Obzorje Evropa, ki jih izvajajo Komisija in države članice na ravni Unije ali nacionalni ravni, prispevati k doseganju ciljev te uredbe.
- (145) K izvajanju te uredbe bi morali prispevati platforma za UI na zahtevo, evropska vozlišča za digitalne inovacije ter centri za testiranje in eksperimentiranje, ki so jih vzpostavile Komisija in države članice na ravni Unije ali nacionalni ravni, in sicer da bi čim bolj zmanjšali tveganja za izvajanje, ki so posledica pomanjkanja znanja in strokovnega znanja na trgu, ter da bi ponudnikom, predvsem MSP, vključno z zagonskimi podjetji, in priglašnim organom olajšali izpolnjevanje njihovih obveznosti iz te uredbe. Platforma za UI na zahtevo, evropska vozlišča za digitalne inovacije ter centri za preskušanje in eksperimentiranje lahko ponudnikom in priglašnim organom v okviru svojih mandatov in pristojnosti zagotavljajo zlasti tehnično in znanstveno podporo.

- (146) Poleg tega je zaradi majhnosti nekaterih operaterjev in da se zagotovi sorazmernost, kar zadeva stroške inovacij, primerno, da se mikropodjetjem omogoči izpolnjevanje ene od najdražjih obveznosti, tj. vzpostavitve sistema upravljanja kakovosti, na poenostavljen način, kar bi zmanjšalo upravno breme in stroške za ta podjetja in ne bi vplivalo na raven varstva in potrebo po skladnosti z zahtevami za visokotvegane sisteme UI. Komisija bi morala pripraviti smernice za opredelitev elementov sistema upravljanja kakovosti, ki jih morajo mikropodjetja izpolnjevati na ta poenostavljen način.
- (147) Primerno je, da Komisija organom, skupinam ali laboratorijem, ustanovljenim ali akreditiranim na podlagi katere koli ustrezne harmonizacijske zakonodaje Unije, ki izpolnjujejo naloge v okviru ugotavljanja skladnosti proizvodov ali pripomočkov, zajetih v navedeni harmonizacijski zakonodaji Unije, čim bolj olajša dostop do centrov za testiranje in eksperimentiranje. To velja zlasti za strokovne odbore, strokovne laboratorije in referenčne laboratorije na področju medicinskih pripomočkov na podlagi uredb (EU) 2017/745 in (EU) 2017/746.

(148) S to uredbo bi bilo treba vzpostaviti okvir upravljanja, ki bi omogočal tako usklajevanje uporabe te uredbe in podporo uporabi na nacionalni ravni kot tudi krepitev zmogljivosti na ravni Unije in sodelovanje deležnikov s področja UI. Za učinkovito izvajanje in izvrševanje te uredbe je potreben okvir upravljanja, ki omogoča usklajevanje in pridobivanje centraliziranega strokovnega znanja na ravni Unije. Urad za UI je bil ustanovljen s sklepom Komisije⁴⁵ z mandatom razvijati strokovno znanje in zmogljivosti Unije na področju UI ter prispevati k izvajanju prava Unije o umetni inteligenci. Države članice bi morale olajšati naloge Urada za UI, da bi podpirale razvoj strokovnega znanja in zmogljivosti Unije na ravni Unije ter okrepile delovanje enotnega digitalnega trga. Poleg tega bi bilo treba ustanoviti odbor, sestavljen iz predstavnikov držav članic, znanstveni odbor za vključitev znanstvene skupnosti in svetovalni forum, da se omogoči prispevanje deležnikov k izvajanju te uredbe na ravni Unije in nacionalni ravni. Razvoj strokovnega znanja in zmogljivosti Unije bi moral vključevati tudi uporabo obstoječih virov in strokovnega znanja, zlasti s pomočjo sinergij s strukturami, vzpostavljenimi v okviru izvrševanja drugega prava na ravni Unije, in sinergij s povezanimi pobudami na ravni Unije, kot so Skupno podjetje EuroHPC ter centri za testiranje in eksperimentiranje na področju UI v okviru programa Digitalna Evropa.

⁴⁵ Sklep Komisije z dne 24. januarja 2024 o ustanovitvi Evropskega urada za umetno inteligenco C(2024) 390 final.

- (149) Da bi omogočili nemoteno, učinkovito in harmonizirano izvajanje te uredbe, bi bilo treba ustanoviti Odbor. Odbor bi moral odražati različne interese ekosistema UI in sestavljati bi ga morali predstavniki držav članic. Odgovoren bi moral biti za številne svetovalne naloge, med drugim za izdajanje mnenj, priporočil in nasvetov ali za prispevanje k dajanju smernic o zadevah, povezanih z izvajanjem te uredbe, vključno z zadevami glede izvrševanja, tehničnimi specifikacijami ali obstoječimi standardi v zvezi z zahtevami iz te uredbe, ter za svetovanje Komisiji ter državam članicam in njihovim pristojnim nacionalnim organom pri posebnih vprašanjih v zvezi z UI. Da bi državam članicam omogočili nekaj prožnosti pri imenovanju njihovih predstavnikov v Odbor, so lahko ti predstavniki katere koli osebe, ki pripadajo javnim subjektom, ter bi morale imeti ustrezne pristojnosti in pooblastila za lažje usklajevanje na nacionalni ravni in prispevanje k izpolnjevanju nalog Odbora. Odbor bi moral ustanoviti dve stalni podskupini, da bi zagotovili platformo za sodelovanje in izmenjavo med organi za nadzor trga in prigrasitvenimi organi o vprašanjih, povezanih z nadzorom trga oziroma priglasiženimi organi. Stalna podskupina za nadzor trga bi morala delovati kot skupina za upravno koordinacijo (ADCO) za to uredbo v smislu člena 30 Uredbe (EU) 2019/1020. V skladu s členom 33 navedene uredbe bi morala Komisija podpirati dejavnosti stalne podskupine za nadzor trga z ocenjevanji ali študijami trga, zlasti z namenom opredelitve vidikov te uredbe, pri katerih je potrebno posebno in nujno usklajevanje med organi za nadzor trga. Odbor lahko ustanovi druge stalne aličasne podskupine za preučitev posebnih vprašanj. Po potrebi bi moral sodelovati tudi z ustreznimi organi, strokovnimi skupinami in mrežami Unije, dejavnimi v okviru ustreznega prava Unije, zlasti tudi s tistimi, dejavnimi na podlagi ustreznega prava Unije o podatkih, digitalnih proizvodih in storitvah.

- (150) Za zagotavljanje sodelovanja deležnikov pri izvajanju in uporabi te uredbe, bi bilo treba vzpostaviti svetovalni forum, ki bi Odboru in Komisiji svetoval in jima zagotavljal tehnično strokovno znanje. Da bi zagotovili raznoliko in uravnoteženo zastopanost deležnikov glede na komercialne in nekomercialne interese, znotraj kategorije poslovnih interesov pa v zvezi z MSP in drugimi podjetji, bi moral biti svetovalni forum med drugim sestavljen iz predstavnikov industrije, zagonskih podjetij, MSP, akademskih krogov, civilne družbe, vključno s socialnimi partnerji, pa tudi Agencije za temeljne pravice, ENISA, Evropskega odbora za standardizacijo (CEN), Evropskega odbora za elektrotehniško standardizacijo (CENELEC) in Evropskega inštituta za telekomunikacijske standarde (ETSI).
- (151) Za podporo izvajanju in izvrševanju te uredbe, zlasti dejavnosti spremljanja, ki jih v zvezi z modeli UI za splošne namene izvaja Urad za UI, bi bilo treba ustanoviti znanstveni odbor neodvisnih strokovnjakov. Neodvisni strokovnjaki, ki sestavljajo znanstveni odbor, bi morali biti izbrani zaradi najnovejšega znanstvenega ali tehničnega strokovnega znanja na področju UI in bi morali svoje naloge opravljati nepristransko in objektivno ter zagotavljati zaupnost informacij in podatkov, pridobljenih pri izvajanju njihovih nalog in dejavnosti. Da bi omogočili okrepitev nacionalnih zmogljivosti, potrebnih za učinkovito izvrševanje te uredbe, bi morale imeti države članice možnost, da strokovnjake, ki sestavljajo znanstveni odbor, zaprosijo, da jim pomagajo pri dejavnostih izvrševanja.

- (152) Da bi podprli ustrezno izvrševanje v zvezi s sistemi UI in okrepili zmogljivosti držav članic, bi bilo treba vzpostaviti podporne strukture Unije za testiranje UI in jih dati na voljo državam članicam.
- (153) Države članice imajo ključno vlogo pri uporabi in izvrševanju te uredbe. V zvezi s tem bi morala vsaka država članica za pristojne nacionalne organe za namen nadzora uporabe in izvajanja te uredbe imenovati vsaj en priglasitveni organ in vsaj en organ za nadzor trga. Države članice se lahko v skladu s svojimi specifičnimi nacionalnimi organizacijskimi značilnostmi in potrebami odločijo, da za opravljanje nalog pristojnih nacionalnih organov v smislu te uredbe imenujejo kateri koli javni subjekt. Da bi na strani držav članic izboljšali učinkovitost organizacije ter vzpostavili enotno kontaktno točko za stike z javnostjo in drugimi partnerji na ravni držav članic in Unije, bi morala vsaka država članica imenovati organ za nadzor trga, ki deluje kot enotna kontaktna točka.
- (154) Pristojni nacionalni organi bi svoja pooblastila morali izvajati neodvisno, nepristransko in brez predsodkov, da bi zaščitili objektivnost svojih dejavnosti in nalog ter zagotovili uporabo in izvajanje te uredbe. Člani teh organov bi se morali vzdržati vseh dejanj, ki niso združljiva z njihovimi dolžnostmi, in zanje bi se morala uporabljati pravila o zaupnosti na podlagi te uredbe.

- (155) Da bi zagotovili, da ponudniki visokotveganih sistemov UI izkušnje pri uporabi visokotveganih sistemov UI lahko upoštevajo za izboljšanje svojih sistemov ter postopka zasnov in razvoja ali da lahko pravočasno izvedejo morebitne popravne ukrepe, bi morali imeti vsi ponudniki vzpostavljen sistem spremljanja po dajanju na trg. Po potrebi bi spremljanje po dajanju na trg moralo vključevati analizo interakcije z drugimi sistemi UI, tudi drugimi napravami in programsko opremo. V spremljanje po dajanju na trg ne bi smeli biti zajeti občutljivi operativni podatki uvajalcev, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Ta sistem je tudi ključen za zagotovitev učinkovitejše in pravočasnejše obravnave morebitnih tveganj, ki izhajajo iz sistemov UI, ki se po dajanju na trg ali v uporabo še naprej „učijo“. V zvezi s tem bi bilo treba od ponudnikov zahtevati tudi, da imajo vzpostavljen sistem za poročanje ustreznim organom o vseh resnih incidentih, ki so posledica uporabe njihovih sistemov UI, tj. incidentih ali okvarah, ki povzročijo smrt ali resno ogroženost zdravja, hude in nepopravljive motnje v upravljanju in delovanju kritične infrastrukture, kršitve obveznosti na podlagi prava Unije o zaščiti temeljnih pravic ali hudo škodo premoženju ali okolju.

- (156) Za zagotovitev ustreznega in učinkovitega izvrševanja zahtev in obveznosti iz te uredbe, ki je harmonizacijska zakonodaja Unije, bi bilo treba v celoti uporabljati sistem nadzora trga in skladnosti proizvodov, vzpostavljen z Uredbo (EU) 2019/1020. Organi za nadzor trga, imenovani na podlagi te uredbe, bi morali imeti vsa izvršilna pooblastila, določena v tej uredbi in Uredbi (EU) 2019/1020, ter bi morali svoja pooblastila in dolžnosti izvajati neodvisno, nepristransko in brez predsodkov. Čeprav za večino sistemov UI ne veljajo posebne zahteve in obveznosti iz te uredbe, lahko organi za nadzor trga sprejmejo ukrepe v zvezi z vsemi sistemi UI, če ti predstavljajo tveganje v skladu s to uredbo. Zaradi posebne narave institucij, agencij in organov Unije, ki spadajo na področje uporabe te uredbe, je za organ za nadzor trga, ki bo pristojen zanje, primerno imenovati Evropskega nadzornika za varstvo podatkov. To ne bi smelo posegati v imenovanje pristojnih nacionalnih organov s strani držav članic. Dejavnosti nadzora trga ne bi smele vplivati na zmožnost nadzorovanih subjektov, da svoje naloge opravljajo neodvisno, kadar je taka neodvisnost zahtevana po pravu Unije.

(157) Ta uredba ne posega v pristojnosti, naloge, pooblastila in neodvisnost ustreznih nacionalnih javnih organov ali teles, ki nadzorujejo uporabo prava Unije o varstvu temeljnih pravic, tudi ne organov za enakost in organov za varstvo podatkov. Kadar je to potrebno za njihov mandat, bi morali imeti navedeni nacionalni javni organi ali telesa tudi dostop do kakršne koli dokumentacije, pripravljene na podlagi te uredbe. Določiti bi bilo treba poseben zaščitni postopek za zagotavljanje ustreznega in pravočasnega izvrševanja v zvezi s sistemi UI, ki predstavljajo tveganje za zdravje, varnost in temeljne pravice. Postopek za take sisteme UI, ki predstavljajo tveganje, bi bilo treba uporabljati za visokotvegane sisteme UI, ki predstavljajo tveganje, prepovedane sisteme, ki so bili dani na trg ali v uporabo oziroma se uporabljajo v skladu s prepovedanimi praksami iz te uredbe, in sisteme UI, ki predstavljajo tveganje in katerih dostopnost je bila omogočena v nasprotju z zahtevami glede preglednosti iz te uredbe.

- (158) Pravo Unije o finančnih storitvah vključuje pravila in zahteve glede notranjega upravljanja in obvladovanja tveganj, ki veljajo za regulirane finančne institucije med opravljanjem teh storitev, tudi kadar uporabljajo sisteme UI. Za zagotovitev usklajene uporabe in izvrševanja obveznosti na podlagi te uredbe ter ustreznih pravil in zahtev iz pravnih aktov Unije o finančnih storitvah bi bilo treba pristojne organe za nadzor in izvrševanje navedenih pravnih aktov, zlasti pristojne organe, opredeljene v Uredbi (EU) št. 575/2013 Evropskega parlamenta in Sveta⁴⁶ ter direktivah 2008/48/ES⁴⁷, 2009/138/ES⁴⁸, 2013/36/EU⁴⁹, 2014/17/EU⁵⁰ in (EU) 2016/97⁵¹ Evropskega parlamenta in Sveta, glede na njihove zadevne pristojnosti imenovati za pristojne organe za namen nadzora izvajanja te uredbe, vključno z dejavnostmi nadzora trga, v zvezi s sistemi UI, ki jih zagotavljajo ali uporabljajo regulirane in nadzorovane finančne institucije, razen če se država članica ne odloči, da bo za opravljanje teh nalog nadzora trga imenovala drug organ.

⁴⁶ Uredba (EU) št. 575/2013 Evropskega parlamenta in Sveta z dne 26. junija 2013 o bonitetnih zahtevah za kreditne institucije in o spremembi Uredbe (EU) št. 648/2012 (UL L 176, 27.6.2013, str. 1).

⁴⁷ Direktiva 2008/48/ES Evropskega parlamenta in Sveta z dne 23. aprila 2008 o potrošniških kreditnih pogodbah in razveljavitvi Direktive Sveta 87/102/EGS (UL L 133, 22.5.2008, str. 66).

⁴⁸ Direktiva 2009/138/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009 o začetku opravljanja in opravljanju dejavnosti zavarovanja in pozavarovanja (Solventnost II) (UL L 335, 17.12.2009, str. 1).

⁴⁹ Direktiva 2013/36/EU Evropskega parlamenta in Sveta z dne 26. junija 2013 o dostopu do dejavnosti kreditnih institucij in bonitetnem nadzoru kreditnih institucij, spremembi Direktive 2002/87/ES ter razveljavitvi direktiv 2006/48/ES in 2006/49/ES (UL L 176, 27.6.2013, str. 338).

⁵⁰ Direktiva 2014/17/EU Evropskega parlamenta in Sveta z dne 4. februarja 2014 o potrošniških kreditnih pogodbah za stanovanjske nepremičnine in spremembi direktiv 2008/48/ES in 2013/36/EU ter Uredbe (EU) št. 1093/2010 (UL L 60, 28.2.2014, str. 34).

⁵¹ Direktiva (EU) 2016/97 Evropskega parlamenta in Sveta z dne 20. januarja 2016 o distribuciji zavarovalnih produktov (UL L 26, 2.2.2016, str. 19).

Ti pristojni organi bi morali imeti vsa pooblastila na podlagi te uredbe in Uredbe (EU) 2019/1020 za izvrševanje zahtev in obveznosti iz te uredbe, vključno s pooblastili za izvajanje naknadnih dejavnosti nadzora trga, ki jih lahko, če je to primerno, vključijo v svoje obstoječe nadzorne mehanizme in postopke na podlagi zadevnega prava Unije o finančnih storitvah. Primerno je predvideti, da bi morali nacionalni organi, ki so odgovorni za nadzor kreditnih institucij, ki jih ureja Direktiva 2013/36/EU, in sodelujejo v enotnem mehanizmu nadzora, vzpostavljenem z Uredbo Sveta (EU) št. 1024/2013⁵², kadar delujejo kot organi za nadzor trga na podlagi te uredbe, Evropski centralni banki nemudoma sporočiti vse informacije, pridobljene v okviru njihovih dejavnosti nadzora trga, ki bi lahko bile zanimive za naloge bonitetnega nadzora Evropske centralne banke, kot so določene v navedeni uredbi. Za nadaljnjo krepitev skladnosti med to uredbo in pravili, ki se uporabljajo za kreditne institucije, ki jih ureja Direktiva 2013/36/EU, je primerno v obstoječe obveznosti in postopke iz Direktive 2013/36/EU vključiti tudi nekatere postopkovne obveznosti ponudnikov v zvezi z obvladovanjem tveganj, spremljanjem po dajanju na trg ter dokumentacijo. Da bi se izognili prekrivanju, bi bilo treba predvideti tudi omejena odstopanja v zvezi s sistemom ponudnikov za upravljanje kakovosti in obveznostjo spremljanja, naloženo uvajalcem visokotveganih sistemov UI, če se ta uporabljajo za kreditne institucije, ki jih ureja Direktiva 2013/36/EU. Isto ureditev bi bilo treba uporabljati za zavarovalnice in pozavarovalnice ter zavarovalne holdinge na podlagi Direktive 2009/138/ES in zavarovalne posrednike na podlagi Direktive (EU) 2016/97 ter druge vrste finančnih institucij, za katere veljajo zahteve glede notranjega upravljanja, ureditev ali postopkov, vzpostavljenih na podlagi ustreznega prava Unije o finančnih storitvah, da se zagotovita doslednost in enaka obravnava v finančnem sektorju.

⁵² Uredba Sveta (EU) št. 1024/2013 z dne 15. oktobra 2013 o prenosu posebnih nalog, ki se nanašajo na politike bonitetnega nadzora kreditnih institucij, na Evropsko centralno banko (UL L 287, 29.10.2013, str. 63).

- (159) Vsak organ za nadzor trga za visokotvegane sisteme UI na področju biometrike, kot so navedeni v eni od prilog k tej uredbi, če se ti sistemi uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja ali za pravosodje in demokratične procese, bi moral imeti pooblastila za preiskovanje in popravne ukrepe, vključno vsaj s pooblastilom za pridobitev dostopa do vseh osebnih podatkov, ki se obdelujejo, in do vseh informacij, potrebnih za opravljanje njegovih nalog. Organi za nadzor trga bi morali imeti možnost, da svoja pooblastila izvajajo popolnoma neodvisno. Morebitne omejitve njihovega dostopa do občutljivih operativnih podatkov na podlagi te uredbe ne bi smele posegati v pooblastila, ki so jim podeljena z Direktivo (EU) 2016/680. Nobena izključitev glede razkritja podatkov nacionalnim organom za varstvo podatkov na podlagi te uredbe ne bi smela vplivati na sedanja ali prihodnja pooblastila teh organov zunaj področja uporabe te uredbe.
- (160) Organom za nadzor trga in Komisiji bi moralo biti omogočeno, da predlagajo skupne dejavnosti – vključno s skupnimi preiskavami, ki jih izvajajo organi za nadzor trga sami ali skupaj s Komisijo –, katerih cilj je spodbujanje skladnosti, odkrivanje neskladnosti, ozaveščanje ali zagotavljanje smernic v zvezi s to uredbo, kar zadeva posebne kategorije visokotveganih sistemov UI, za katere se ugotovi, da predstavljajo resno tveganje v dveh ali več državah članicah. Skupne dejavnosti za spodbujanje skladnosti bi bilo treba izvajati v skladu s členom 9 Uredbe (EU) 2019/1020. Urad za UI bi moral zagotavljati usklajevalno podporo za skupne preiskave.

- (161) Pojasniti je treba odgovornosti in pristojnosti na ravni Unije in nacionalni ravni v zvezi z sistemi UI, ki temeljijo na modelih UI za splošne namene. Da bi se izognili prekrivanju pristojnosti, kadar sistem UI temelji na modelu UI za splošne namene ter kadar model in sistem zagotavlja isti ponudnik, bi moral biti za nadzor na ravni Unije pristojen Urad za UI, ki bi moral v ta namen imeti pooblastila organa za nadzor trga v smislu Uredbe (EU) 2019/1020. V vseh drugih primerih so za nadzor sistemov UI še naprej odgovorni nacionalni organi za nadzor trga. Vendar bi morali organi za nadzor trga za sisteme UI za splošne namene, ki jih lahko uvajalci neposredno uporabljajo za vsaj en namen, ki je razvrščen kot visoko tveganje, sodelovati z Urdom za UI pri izvedbi ocen skladnosti ter o tem ustrezno obvestiti Odbor in druge organe za nadzor trga. Poleg tega bi morali imeti organi za nadzor trga možnost, da Urad za UI zaprosijo za pomoč, kadar organ za nadzor trga ne more zaključiti preiskave visokotveganega sistema UI, ker ne more dostopati do nekaterih informacij, ki se nanašajo na model UI za splošne namene, na katerem temelji visokotvegani sistem UI. V takih primerih bi se moral smiselno uporabljati postopek v zvezi s čezmejno medsebojno pomočjo iz poglavja VI Uredbe (EU) 2019/1020.

- (162) Da bi na ravni Unije čim boljše izkoristili centralizirano strokovno znanje in sinergije Unije, bi morala biti pooblastila za nadzor in izvrševanje obveznosti za ponudnike modelov UI za splošne namene v pristojnosti Komisije. Urad za UI bi moral imeti možnost, da izvede vse potrebne ukrepe za spremljanje učinkovitega izvajanja te uredbe v zvezi z modeli UI za splošne namene. Imeti bi moral možnost, da na lastno pobudo na podlagi rezultatov njegovih dejavnosti spremljanja ali na zahtevo organov za nadzor trga v skladu s pogoji iz te uredbe razišče morebitne kršitve pravil o ponudnikih modelov UI za splošne namene. Da bi podprli učinkovito spremljanje Urada za UI, bi bilo treba določiti možnost, da lahko ponudniki nižje v verigi vložijo pritožbe zaradi morebitnih kršitev pravil o ponudnikih modelov UI za splošne namene in sistemov UI.
- (163) Da bi dopolnili sisteme upravljanja modelov UI za splošne namene, bi moral znanstveni odbor prispevati k dejavnostim spremljanja Urada za UI, ki mu v nekaterih primerih lahko pošlje kvalificirana opozorila, ki sprožijo nadaljnje ukrepanje, kot so preiskave. To bi se moralo zgoditi, kadar znanstveni odbor utemeljeno sumi, da model UI za splošne namene predstavlja konkretno in prepoznavno tveganje na ravni Unije. To bi se prav tako moralo zgoditi, kadar znanstveni odbor utemeljeno sumi, da model UI za splošne namene izpolnjuje merila, na podlagi katerih bi moral biti razvrščen kot model UI za splošne namene s sistemskim tveganjem. Da se znanstvenemu svetu zagotovijo informacije, potrebne za opravljanje teh nalog, bi moral obstajati mehanizem, s katerim lahko znanstveni odbor zaprosi Komisijo, da od ponudnika zahteva dokumentacijo ali informacije.

- (164) Urad za UI bi moral imeti možnost, da sprejme potrebne ukrepe za spremljanje učinkovitega izvajanja in izpolnjevanja obveznosti za ponudnike modelov UI za splošne namene iz te uredbe. Urad za UI bi moral imeti možnost, da razišče morebitne kršitve v skladu s pooblastili na podlagi te uredbe, tudi tako, da zahteva dokumentacijo in informacije, izvaja ocenjevanje ter od ponudnikov modelov UI za splošne namene zahteva ukrepe. Pri izvajanju ocenjevanja in zato, da bi uporabili neodvisno strokovno znanje, bi moral Urad za UI imeti možnost vključiti neodvisne strokovnjake, da v njegovem imenu izvedejo ocenjevanje. Izpolnjevanje obveznosti bi moralo biti izvršljivo, med drugim z zahtevami za sprejetje ustreznih ukrepov, vključno z ukrepi za zmanjšanje tveganja v primeru prepoznanih sistemskih tveganj, ter z omejevanjem omogočanja dostopnosti modela na trgu, njegovim umikom ali odpoklicem. Kot zaščitni ukrepi, kadar je to potrebno poleg procesnih pravic iz te uredbe, bi morali imeti ponudniki modelov UI za splošne namene procesne pravice iz člena 18 Uredbe (EU) 2019/1020, ki bi se morale uporabljati smiselno in brez poseganja v bolj specifične procesne pravice iz te uredbe.

(165) Razvoj sistemov UI, ki niso visokotvegani sistemi UI, v skladu z zahtevami iz te uredbe lahko pripelje do večjega koriščenja etične in zaupanja vredne UI v Uniji. Ponudnike sistemov UI, ki niso sistemi visokega tveganja, bi bilo treba spodbujati k oblikovanju kodeksov ravnanja, vključno s povezanimi mehanizmi upravljanja, ki bodo namenjeni spodbujanju prostovoljne uporabe nekaterih ali vseh obveznih zahtev, ki se uporabljajo za visokotvegane sisteme UI, prilagojeni predvidenemu namenu sistemov in manjšemu tveganju ter bodo v njih upoštevane razpoložljive tehnične rešitve in najboljše prakse v industriji, kot so modeli in podatkovne kartice. Ponudnike in po potrebi uvajalce vseh sistemov UI, ne glede na to, ali so sistemi visokega tveganja ali ne, in modelov UI bi bilo treba spodbujati tudi k prostovoljni uporabi dodatnih zahtev, povezanih na primer z elementi etičnih smernic Unije za zaupanja vredno UI, okoljsko trajnostnostjo, ukrepi za pismenost na področju UI, zasnovo in razvojem sistemov UI, ki zagotavljata inkluzivnost in raznolikost, vključno s poudarkom na ranljivih osebah in dostopnostjo za invalide, sodelovanjem deležnikov, po potrebi s sodelovanjem ustreznih deležnikov, kot so podjetja in organizacije civilne družbe, akademski krogi, raziskovalne organizacije, sindikati in organizacije za varstvo potrošnikov, pri zasnovi in razvoju sistemov UI, ter z raznolikostjo razvojnih skupin, vključno z uravnoteženo zastopanostjo spolov. Da bi zagotovili učinkovitost prostovoljnih kodeksov ravnanja, bi morali ti temeljiti na jasnih ciljih in ključnih kazalnikih uspešnosti za merjenje doseganja teh ciljev. Prav tako bi jih bilo treba razvijati na inkluziven način, kot je ustrezno, ob sodelovanju ustreznih deležnikov, kot so podjetja in organizacije civilne družbe, akademski krogi, raziskovalne organizacije, sindikati in organizacije za varstvo potrošnikov. Komisija lahko pripravi pobude, tudi sektorske narave, da se omogoči zmanjšanje tehničnih ovir za čezmejno izmenjavo podatkov za razvoj UI, tudi na infrastrukturi za dostop do podatkov, ter semantično in tehnično interoperabilnost različnih vrst podatkov.

- (166) Pomembno je, da so sistemi UI, ki so povezani s proizvodi brez visokega tveganja v skladu s to uredbo in jim zato ni treba izpolnjevati zahtev za visokotvegane sisteme UI, kljub temu varni, ko so dani na trg ali v uporabo. Da bi prispevali k temu cilju, bi se Uredba (EU) 2023/988 Evropskega parlamenta in Sveta⁵³ uporabljala kot varnostna mreža.
- (167) Za zagotovitev zaupanja vrednega in konstruktivnega sodelovanja pristojnih organov na ravni Unije in nacionalni ravni bi morale vse strani, ki sodelujejo pri uporabi te uredbe, spoštovati zaupnost informacij in podatkov, ki so jih pridobili pri opravljanju svojih nalog, v skladu s pravom Unije ali nacionalnim pravom. Svoje naloge in dejavnosti bi morali opravljati tako, da varujejo zlasti pravice intelektualne lastnine, zaupne poslovne informacije in poslovne skrivnosti, učinkovito izvajanje te uredbe, javne in nacionalne varnostne interese, celovitost kazenskih in upravnih postopkov ter celovitost tajnih podatkov.

⁵³ Uredba (EU) 2023/988 Evropskega parlamenta in Sveta z dne 10. maja 2023 o splošni varnosti proizvodov, spremembi Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta in Direktive (EU) 2020/1828 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2001/95/ES Evropskega parlamenta in Sveta in Direktive Sveta 87/357/EGS (UL L 135, 23.5.2023, str. 1).

- (168) Skladnost s to uredbo bi morala biti izvršljiva z naložitvijo kazni in drugimi izvršilnimi ukrepi. Države članice bi morale sprejeti vse potrebne ukrepe za zagotovitev izvajanja določb te uredbe, tudi z določitvijo učinkovitih, sorazmernih in odvračilnih kazni za njihovo kršitev, in za upoštevanje načela ne bis in idem. Za okrepitev in usklajitev upravnih kazni za kršitev te uredbe bi bilo treba določiti zgornje meje za določitev upravnih glob za nekatere posebne kršitve. Države članice bi morale pri določanju višine glob v vsakem posameznem primeru upoštevati vse ustrezne okoliščine konkretne situacije, zlasti pa naravo, težo in trajanje kršitve ter njene posledice in velikost ponudnika, zlasti če je ponudnik MSP, vključno z zagonskim podjetjem. Evropski nadzornik za varstvo podatkov bi moral biti pooblaščen za nalaganje glob institucijam, agencijam in organom Unije, ki spadajo na področje uporabe te uredbe.
- (169) Izpolnjevanje obveznosti za ponudnike modelov UI za splošne namene, določenih na podlagi te uredbe, bi moralo med drugim biti izvršljivo z globami. V ta namen bi bilo treba določiti tudi ustrezne ravni glob za kršitev navedenih obveznosti, vključno z neizpolnjevanjem ukrepov, ki jih Komisija zahteva v skladu s to uredbo, ob upoštevanju ustreznih zastaralnih rokov v skladu z načelom sorazmernosti. Vse odločitve, ki jih Komisija sprejme na podlagi te uredbe, so podvržene nadzoru Sodišča Evropske unije v skladu s PDEU, vključno z neomejeno pristojnostjo Sodišča glede kazni na podlagi člena 261 PDEU.

- (170) Pravo Unije in nacionalno pravo fizičnim in pravnim osebam, na pravice in svoboščine katerih negativno vpliva uporaba sistemov UI, že zagotavljata učinkovita pravna sredstva. Brez poseganja v ta pravna sredstva lahko pritožbo pri ustreznem organu za nadzor trga vloži vsaka fizična ali pravna oseba, ki upravičeno meni, da je prišlo do kršitve te uredbe.
- (171) Osebe, na katere vpliva uporaba sistemov UI, bi morale imeti pravico do pojasnila, kadar odločitev uvajalca temelji predvsem na izhodnih podatkih nekaterih visokotveganih sistemov UI, ki spadajo na področje uporabe te uredbe, in kadar ima ta odločitev pravne učinke za te osebe ali nanje podobno znatno vpliva na način, za katerega menijo, da ima negativne učinke na njihovo zdravje, varnost in temeljne pravice. To pojasnilo bi moralo biti jasno in smiselno ter temelj, na podlagi katerega osebe, na katere vpliva uporaba sistemov UI, lahko uveljavljajo svoje pravice. Pravica do pojasnila se ne bi smela uporabljati za uporabo sistemov UI, za katere izjeme ali omejitve izhajajo iz prava Unije ali nacionalnega prava, temveč bi se morala uporabljati le, če ta pravica še ni določena na podlagi prava Unije.
- (172) Osebe, ki kot žvižgači opozarjajo na kršitve te uredbe, bi morale biti zaščitene na podlagi prava Unije. Za prijavo kršitev te uredbe in zaščito oseb, ki te kršitve prijavijo, bi se zato morala uporabljati Direktiva (EU) 2019/1937 Evropskega parlamenta in Sveta⁵⁴.

⁵⁴ Direktiva (EU) 2019/1937 Evropskega parlamenta in Sveta z dne 23. oktobra 2019 o zaščiti oseb, ki prijavijo kršitve prava Unije (UL L 305, 26.11.2019, str. 17).

(173) Za zagotovitev, da se regulativni okvir lahko po potrebi prilagodi, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 PDEU sprejme akte za spremembo pogojev, pod katerimi se sistem UI ne sme šteti za sistem visokega tveganja, seznama visokotveganih sistemov UI, določb o tehnični dokumentaciji, vsebine EU izjave o skladnosti, določb o postopkih ugotavljanja skladnosti, določb o vzpostavitvi visokotveganih sistemov UI, za katere bi se moral uporabljati postopek ugotavljanja skladnosti na podlagi ocene sistema upravljanja kakovosti in ocene tehnične dokumentacije, praga, meril uspešnosti in kazalnikov, tudi z njihovo dopolnitvijo, kot so opredeljeni v pravilih za razvrščanje modelov UI za splošne namene s sistemskim tveganjem, meril za označevanje modelov UI za splošne namene s sistemskim tveganjem, tehnične dokumentacije za ponudnike modelov UI za splošne namene in informacij o preglednosti za ponudnike modelov UI za splošne namene. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, tudi na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje⁵⁵. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njihovi strokovnjaki pa se lahko sistematično udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov.

⁵⁵ UL L 123, 12.5.2016, str. 1.

- (174) Glede na hiter tehnološki razvoj in tehnično strokovno znanje, potrebno za učinkovito izvajanje te uredbe bi morala Komisija oceniti in pregledati to uredbo do ... [pet let od datuma začetka veljavnosti te uredbe] in nato vsaka štiri leta ter poročati Evropskemu parlament in Svetu. Poleg tega bi morala Komisija ob upoštevanju posledic za področje uporabe te uredbe enkrat letno oceniti potrebo po spremembi seznama visokotveganih sistemov UI in seznama prepovedanih praks. Komisija bi morala do ... [štiri leta od datuma začetka veljavnosti te uredbe] in nato vsaka štiri leta oceniti tudi potrebo po spremembi seznama področij z visokim tveganjem iz ene od prilog k tej uredbi, sisteme UI, ki spadajo na področje uporabe obveznosti glede preglednosti, učinkovitost sistema nadzora in upravljanja ter napredek pri razvoju standardizacijskih dokumentov o energetsko učinkovitem razvoju modelov UI za splošno rabo, vključno s potrebo po nadaljnjih ukrepih ali dejavnostih, ter o tem poročati Evropskemu parlamentu in Svetu. Komisija bi morala do ... [štiri leta od datuma začetka veljavnosti te uredbe] ter nato vsaka tri leta oceniti učinek in učinkovitost prostovoljnih kodeksov ravnanja za spodbujanje uporabe zahtev, ki veljajo za visokotvegane sisteme UI, za sisteme UI, ki niso visokotvegani sistemi UI, ter morebitnih drugih dodatnih zahtev za takšne sisteme UI.

- (175) Da se zagotovijo enotni pogoji za izvajanje te uredbe, bi bilo treba na Komisijo prenesti izvedbena pooblastila. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta⁵⁶.
- (176) Ker cilja te uredbe, in sicer izboljšati delovanje notranjega trga in spodbujati uvajanje na človeka osredotočene in zaupanja vredne UI, ob zagotavljanju visoke ravni varovanja zdravja, varnosti, temeljnih pravic iz Listine, vključno z demokracijo, pravno državo in varstvom okolja, pred škodljivimi učinki sistemov UI v Uniji ter podpiranju inovacij, države članice ne morejo zadovoljivo doseči, temveč se zaradi obsega ali učinka ukrepa lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 PEU. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

⁵⁶ Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

- (177) Da se zagotovita pravna varnost in ustrezno prilagoditveno obdobje za operaterje ter preprečijo motnje na trgu, vključno z zagotavljanjem neprekinjene uporabe sistemov UI, je primerno, da se ta uredba uporablja za visokotvegane sisteme UI, ki so bili dani na trg ali v uporabo pred splošnim datumom začetka njene uporabe, le, če se pri navedenih sistemih z navedenim datumom bistveno spremeni njihova zasnova ali predvideni namen. Primerno je pojasniti, da bi bilo treba v zvezi s tem koncept bistvene spremembe razumeti kot vsebinsko enakovreden pojmu bistvene spremembe, ki se uporablja samo za visokotvegane sisteme UI na podlagi te uredbe. Tako upravljavci sistemov UI, ki so komponente obsežnih informacijskih sistemov, vzpostavljenih s pravnimi akti iz ene od prilog k tej uredbi, kot tudi operaterji visokotveganih sistemov UI, ki naj bi jih uporabljali javni organi, bi morali izjemoma in glede na javno odgovornost sprejeti potrebne ukrepe za doseg skladnosti z zahtevami iz te uredbe do konca leta 2030 oziroma do ... [šest let od datuma začetka veljavnosti te uredbe].
- (178) Ponudnike visokotveganih sistemov UI se spodbuja, da že v prehodnem obdobju začnejo prostovoljno izpolnjevati ustrezne obveznosti iz te uredbe.

- (179) Ta uredba se uporablja od ... [dve leti od datuma začetka veljavnosti te uredbe]. Vendar bi bilo treba zaradi nesprejemljivega tveganja, povezanega z uporabo UI na določene načine, prepovedi ter splošne določbe te uredbe uporabljati že od ... [šest mesecev od datuma začetka veljavnosti te uredbe]. Čeprav bodo te prepovedi polno učinkovale šele po vzpostavitvi upravljanja in izvrševanja te uredbe, je pomembno predvideti uporabo prepovedi, da se upoštevajo nesprejemljiva tveganja in zato, da bi to vplivalo na druge postopke, kot denimo v civilnem pravu. Poleg tega bi morala infrastruktura, povezana z upravljanjem in sistemom ugotavljanja skladnosti, začeti delovati pred ... [dve leti od datuma začetka veljavnosti te uredbe], zato bi bilo treba določbe o priglašeni in strukturi upravljanja uporabljati od ... [12 mesecev od datuma začetka veljavnosti te uredbe]. Glede na hiter tehnološki napredek in sprejetje modelov UI za splošne namene bi bilo treba obveznosti za ponudnike modelov UI za splošne namene uporabljati od ... [12 mesecev od datuma začetka veljavnosti te uredbe]. Kodekse prakse bi bilo treba pripraviti najpozneje do ... [devet mesecev od datuma začetka veljavnosti te uredbe], da bi ponudniki lahko pravočasno dokazali skladnost. Urad za UI bi moral zagotavljati posodabljanje pravil in postopkov razvrščanja glede na tehnološki razvoj. Poleg tega bi morale države članice določiti pravila o kaznih, vključno z upravnimi globami, in o njih uradno obvestiti Komisijo ter do datuma začetka uporabe te uredbe zagotoviti, da jih bodo učinkovito izvajale. Zato bi bilo treba določbe o kaznih uporabljati od ... [12 mesecev od datuma začetka veljavnosti te uredbe].

- (180) V skladu s členom 42(1) in (2) Uredbe (EU) 2018/1725 je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov in Evropskim odborom za varstvo podatkov, ki sta dala mnenje 18. junija 2021 –

SPREJELA NASLEDNJO UREDBO:

Poglavje I

Splošne določbe

Člen 1

Predmet urejanja

1. Namen te uredbe je izboljšati delovanje notranjega trga in spodbujati uvajanje na človeka osredotočene in zaupanja vredne umetne inteligence (UI) ter zagotoviti visoko raven varovanja zdravja, varnosti in temeljnih pravic iz Listine, vključno z demokracijo, pravno državo in varstvom okolja, pred škodljivimi učinki sistemov UI v Uniji ter podpirati inovacije.
2. V tej uredbi so določeni:
 - (a) harmonizirana pravila za dajanje na trg, dajanje v uporabo ter za uporabo sistemov UI v Uniji;
 - (b) prepovedi nekaterih praks UI;
 - (c) posebne zahteve za visokotvegane sisteme UI in obveznosti za operaterje takih sistemov;
 - (d) harmonizirana pravila o preglednosti za nekatere sisteme UI;
 - (e) harmonizirana pravila za dajanje na trg modelov UI za splošne namene;

- (f) pravila o spremljanju trga, nadzoru trga, upravljanju in izvrševanju;
- (g) ukrepi v podporo inovacijam s posebnim poudarkom na MSP, vključno z zagonskimi podjetji.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za:

- (a) ponudnike, ki dajejo na trg ali v uporabo sisteme UI ali dajejo na trg modele UI za splošne namene v Uniji, ne glede na to, ali imajo ti ponudniki sedež ali se nahajajo v Uniji ali v tretji državi;
- (b) uvajalce sistemov UI, ki imajo sedež ali se nahajajo v Uniji;
- (c) ponudnike in uvajalce sistemov UI, ki imajo sedež ali se nahajajo v tretji državi, kadar se izhodni podatki, ki jih sistem UI ustvari, uporabljajo v Uniji;
- (d) uvoznike in distributerje sistemov UI;
- (e) proizvajalce proizvodov, ki dajejo sistem UI na trg ali v uporabo skupaj s svojim proizvodom in pod svojim imenom ali znamko;
- (f) pooblašcene zastopnike ponudnikov, ki nimajo sedeža v Uniji;
- (g) osebe, ki jih zadeva in se nahajajo v Uniji.

2. Za sisteme UI, ki so razvrščeni med visoko tvegane sisteme UI v skladu s členom 6(1) v povezavi s proizvodi, zajetimi v harmonizacijski zakonodaji Unije s seznama v Prilogi I, oddelek B, se uporablja samo člen 6(1), členi 102 do 109 in člen 112. Člen 57 se uporablja le, če so bile zahteve za visokotvegane sisteme UI iz te uredbe vključene v to harmonizacijsko zakonodajo Unije.
3. Ta uredba se ne uporablja za področja, ki ne spadajo na področje uporabe prava Unije, in v nobenem primeru ne vpliva na pristojnosti držav članic v zvezi z nacionalno varnostjo, ne glede na vrsto subjekta, ki ga države članice pooblastijo za opravljanje nalog v zvezi s temi pristojnostmi.

Ta uredba se ne uporablja za sisteme UI, kadar in kolikor so s spremembami ali brez njih dani na trg ali v uporabo oziroma se uporabljajo izključno za vojaške, obrambne ali nacionalne varnostne namene, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

Ta uredba se ne uporablja za sisteme UI, ki niso dani na trg ali v uporabo v Uniji, kadar se izhodni podatki uporabljajo v Uniji izključno za vojaške, obrambne ali nacionalne varnostne namene, ne glede na vrsto subjekta, ki izvaja te dejavnosti.

4. Ta uredba se ne uporablja za javne organe v tretji državi in mednarodne organizacije, ki spadajo na področje uporabe te uredbe na podlagi odstavka 1, kadar ti organi ali organizacije uporabljajo sisteme UI v okviru mednarodnega sodelovanja ali sporazumov za sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter za sodelovanje na področju pravosodja z Unijo ali z eno ali več državami članicami, pod pogojem, da ta tretja država ali mednarodna organizacija zagotovi ustrezne zaščitne ukrepe v zvezi z varstvom temeljnih pravic in svoboščin posameznikov.
5. Ta uredba ne vpliva na uporabo določb o odgovornosti ponudnikov posredniških storitev iz poglavja II Uredbe (EU) 2022/2065.
6. Ta uredba se ne uporablja za sisteme UI ali modele UI, vključno z njihovimi izhodnimi podatki, posebej razvite in dane v uporabo zgolj za namene znanstvenih raziskav in razvoja.
7. Pravo Unije o varstvu osebnih podatkov, zasebnosti in zaupnosti komunikacij se uporablja za osebne podatke, ki se obdelujejo v zvezi s pravicami in obveznostmi iz te uredbe. Brez poseganja v člen 10(5) in člen 59 te uredbe ta uredba ne vpliva na Uredbo (EU) 2016/679 ali (EU) 2018/1725 ali Direktivo 2002/58/ES ali (EU) 2016/680.
8. Ta uredba se ne uporablja za raziskovalne dejavnosti, dejavnosti testiranja ali razvojne dejavnosti v zvezi z sistemi UI ali modeli UI, preden se ti dajo na trg ali v uporabo. Te dejavnosti se morajo izvajati v skladu z veljavnim pravom Unije. Ta izključitev ne zajema testiranja v realnih razmerah.

9. Ta uredba ne posega v pravila, določena v drugih pravnih aktih Unije v zvezi z varstvom potrošnikov in varnostjo proizvodov.
10. Ta uredba se ne uporablja za obveznosti uvajalcev, ki so fizične osebe in uporabljajo sisteme UI v okviru povsem osebne nepoklicne dejavnosti.
11. Ta uredba Uniji ali državam članicam ne preprečuje, da ohranijo ali uvedejo zakone ali druge predpise, ki so za delavce ugodnejši v smislu varstva njihovih pravic v zvezi z delodajalčevo uporabo sistemov UI, ali da spodbujajo ali dovolijo uporabo kolektivnih pogodb, ki so za delavce ugodnejše.
12. Ta uredba se ne uporablja za sisteme UI, objavljene na podlagi prostih in odprtokodnih licenc, razen če so dani na trg ali v uporabo kot visokotvegani sistemi UI ali sistem UI iz člena 5 ali 50.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

- (1) „sistem UI“ pomeni sistem temelječ na napravah, ki je zasnovan za delovanje z različnimi stopnjami avtonomije in lahko po uvedbi izkaže prilagodljivost ter za eksplicitne ali implicitne cilje iz prejetih vhodnih podatkov sklepa, kako ustvariti izhodne podatke, kot so napovedi, vsebine, priporočila ali odločitve, ki lahko vplivajo na fizična ali virtualna okolja;

- (2) „tveganje“ pomeni kombinacijo verjetnosti pojava škode in resnosti te škode;
- (3) „ponudnik“ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki razvije sistem UI ali model UI za splošne namene ali ima razvit sistem UI ali model UI za splošne namene in ga da na trg ali da sistem UI v uporabo pod svojim imenom ali znamko, za plačilo ali brezplačno;
- (4) „uvajalec“ pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki sistem UI uporablja v svoji pristojnosti, razen kadar se sistem UI uporablja v okviru osebne nepoklicne dejavnosti;
- (5) „pooblaščen zastopnik“ pomeni fizično ali pravno osebo, ki se nahaja ali ima sedež v Uniji in je od ponudnika sistema UI ali modela UI za splošne namene prejela in sprejela pisno pooblastilo, da v njegovem imenu opravlja in izvaja obveznosti in postopke, določene v tej uredbi;
- (6) „uvoznik“ pomeni fizično ali pravno osebo, ki se nahaja ali ima sedež v Uniji, ki da na trg sistem UI, ki nosi ime ali znamko fizične ali pravne osebe s sedežem v tretji državi;
- (7) „distributer“ pomeni fizično ali pravno osebo v dobavni verigi, razen ponudnika ali uvoznika, ki omogoči dostopnost sistema UI na trgu Unije;
- (8) „operator“ pomeni ponudnika, proizvajalca proizvoda, uvajalca, pooblaščenega zastopnika, uvoznika ali distributerja;

- (9) „dajanje na trg“ pomeni, da je sistem UI ali model UI za splošne namene prvič dostopen na trgu Unije;
- (10) „dostopnost na trgu“ pomeni dobavo sistema UI ali modela UI za splošne namene za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti, bodisi za plačilo ali brezplačno;
- (11) „dajanje v uporabo“ pomeni dobavo sistema UI za prvo uporabo neposredno uvajalcu ali za lastno uporabo v Uniji za predvideni namen;
- (12) „predvideni namen“ pomeni uporabo, za katero je ponudnik namenil sistem UI, vključno s posebnim kontekstom in pogoji uporabe, kot je navedeno v informacijah, ki jih je ponudnik predložil v navodilih za uporabo, v promocijskem ali prodajnem gradivu in izjavah ter v tehnični dokumentaciji;
- (13) „razumno predvidljiva napačna uporaba“ pomeni uporabo sistema UI na način, ki sicer ni v skladu s predvidenim namenom, vendar je lahko posledica razumno predvidljivega človeškega vedenja ali interakcije z drugimi sistemi, vključno z drugimi sistemi UI;
- (14) „varnostna komponenta“ pomeni komponento proizvoda ali sistema UI, ki opravlja varnostno funkcijo za ta proizvod ali sistem UI ali katere nedelovanje ali okvara ogroža zdravje in varnost oseb ali premoženja;
- (15) „navodila za uporabo“ pomeni informacije, ki jih zagotovi ponudnik, da uvajalca obvesti zlasti o predvidenem namenu in pravilni uporabi sistema UI;

- (16) „odpoklic sistema UI“ pomeni vsak ukrep, namenjen zagotovitvi vračila sistema UI, ki je bil na voljo upravljalcem, ponudniku ali namenjen zagotovitvi prenehanja delovanja ali onemogočanja uporabe tega sistema;
- (17) „umik sistema UI“ pomeni vsak ukrep, namenjen preprečevanju dostopnosti sistema UI v dobavni verigi na trgu;
- (18) „zmogljivost sistema UI“ pomeni sposobnost sistema UI, da doseže svoj predvideni namen;
- (19) „priglasitveni organ“ pomeni nacionalni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje;
- (20) „ugotavljanje skladnosti“ pomeni postopek ugotavljanja, ali so izpolnjene zahteve iz poglavja III, oddelek 2, v zvezi z visokotveganim sistemom UI;
- (21) „organ za ugotavljanje skladnosti“ pomeni organ, ki kot tretja stran izvaja dejavnosti ugotavljanja skladnosti, vključno s testiranjem, certificiranjem in kontrolo;
- (22) „priglašeni organ“ pomeni organ za ugotavljanje skladnosti, priglašen v skladu s to uredbo in drugo ustrezno harmonizacijsko zakonodajo Unije;
- (23) „bistvena sprememba“ pomeni spremembo sistema UI po dajanju na trg ali v uporabo, ki ni predvidena ali načrtovana pri prvotnem ugotavljanju skladnosti, ki jo je izvedel ponudnik, in ki posledično vpliva na skladnost sistema UI z zahtevami iz poglavja III, oddelek 2, ali povzroči spremembo predvidenega namena, za katerega je bila skladnost sistema UI ugotavljana;

- (24) „oznaka CE“ pomeni oznako, s katero ponudnik izjavlja, da je sistem UI skladen z zahtevami iz poglavja III, oddelek 2, in druge veljavne harmonizacijske zakonodaje Unije, ki določa njeno namestitvev;
- (25) „sistem spremljanja po dajanju na trg“ pomeni vse dejavnosti, ki jih izvajajo ponudniki sistemov UI, da bi zbirali in pregledovali izkušnje, pridobljene z uporabo sistemov UI, ki jih dajo na trg ali v uporabo, da bi ugotovili, ali so potrebni takojšnji popravni ali preventivni ukrepi;
- (26) „organ za nadzor trga“ pomeni nacionalni organ, ki izvaja dejavnosti in sprejema ukrepe na podlagi Uredbe (EU) 2019/1020;
- (27) „harmonizirani standard“ pomeni harmonizirani standard, kakor je opredeljen v členu 2(1), točka (c), Uredbe (EU) št. 1025/2012;
- (28) „skupna specifikacija“ pomeni sklop tehničnih specifikacij, kakor so opredeljene v členu 2, točka 4, Uredbe (EU) št. 1025/2012 in v katerih je opisano, kako izpolnjevati nekatere zahteve, določene na podlagi te uredbe;
- (29) „učni podatki“ pomeni podatke, ki se uporabljajo za učenje sistema UI s prilagajanjem njegovih učljivih parametrov;
- (30) „validacijski podatki“ pomeni podatke, ki se uporabljajo za ocenjevanje naučenega sistema UI ter za uravnavanje neučljivih parametrov in postopka učenja sistema, med drugim za preprečevanje premajhnega ali prevelikega prilagajanja;

- (31) „nabor validacijskih podatkov“ pomeni ločen nabor podatkov ali fiksni ali spremenljivi del nabora učnih podatkov;
- (32) „testni podatki“ pomeni podatke, ki se uporabljajo za zagotavljanje neodvisne ocene sistema UI za potrditev pričakovane zmogljivosti tega sistema pred dajanjem na trg ali v uporabo;
- (33) „vhodni podatki“ pomeni podatke, ki se vnesejo v sistem UI ali jih ta neposredno pridobi in na podlagi katerih sistem ustvari izhodne podatke;
- (34) „biometrični podatki“ pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi fizične osebe, kot so podoba obraza ali daktiloskopski podatki;
- (35) „biometrična identifikacija“ pomeni avtomatizirano prepoznavanje fizičnih, fizioloških, vedenjskih ali psiholoških lastnosti človeka z namenom ugotavljanja identitete fizične osebe s primerjavo biometričnih podatkov tega posameznika z biometričnimi podatki posameznikov, shranjenimi v podatkovni zbirki;
- (36) „biometrično preverjanje“ pomeni avtomatizirano „ena proti ena“ preverjanje, vključno z avtentikacijo, identitete fizičnih oseb s primerjavo njihovih biometričnih podatkov s predhodno pridobljenimi biometričnimi podatki;
- (37) „posebne vrste osebnih podatkov“ pomeni kategorije osebnih podatkov iz člena 9(1) Uredbe (EU) 2016/679, člena 10 Direktive (EU) 2016/680 in člena 10(1) Uredbe (EU) 2018/1725;

- (38) „občutljivi operativni podatki“ pomeni operativne podatke, povezane z dejavnostmi preprečevanja, odkrivanja, preiskovanja ali pregona kaznivih dejanj, katerih razkritje bi lahko ogrozilo celovitost kazenskih postopkov;
- (39) „sistem za prepoznavanje čustev“ pomeni sistem UI za prepoznavanje čustev ali namenov ali sklepanje o čustvih ali namenih fizičnih oseb na podlagi njihovih biometričnih podatkov;
- (40) „sistem za biometrično kategorizacijo“ pomeni sistem UI za razvrščanje fizičnih oseb v posebne kategorije na podlagi njihovih biometričnih podatkov, razen če gre za pomožni in iz objektivnih tehničnih razlogov nujno potreben sistem druge komercialne storitve;
- (41) „sistem za biometrično identifikacijo na daljavo“ pomeni sistem UI za identifikacijo fizičnih oseb brez njihovega dejavnega sodelovanja, običajno na daljavo, s primerjavo biometričnih podatkov osebe z biometričnimi podatki iz referenčne podatkovne zbirke;
- (42) „sistem za biometrično identifikacijo na daljavo v realnem času“ pomeni sistem za biometrično identifikacijo na daljavo, pri katerem se zajemanje biometričnih podatkov, primerjava in identifikacija izvedejo brez znatnih zamud, ki ne zajema le takojšnje identifikacije, temveč tudi identifikacijo s krajšimi zamiki, da se prepreči izogibanje;
- (43) „sistem za naknadno biometrično identifikacijo na daljavo“ pomeni sistem za biometrično identifikacijo na daljavo, ki ni sistem za biometrično identifikacijo na daljavo v realnem času;

- (44) „javno dostopen prostor“ pomeni vsak fizični prostor v javni ali zasebni lasti, ki je dostopen nedoločenemu številu fizičnih oseb, ne glede na to, ali se lahko uporabljajo določeni pogoji za dostop, in ne glede na morebitne omejitve kapacitete;
- (45) „organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“ pomeni:
- (a) kateri koli javni organ, ki je pristojen za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, ali
 - (b) kateri koli drug organ ali subjekt, ki v skladu s pravom države članice lahko opravlja javne funkcije in izvaja javna pooblastila za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;
- (46) „preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“ pomeni dejavnosti, ki jih organi za preprečevanje, odkrivanje ali preiskovanje kaznivih dejanj izvajajo ali se izvajajo v njihovem imenu za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;
- (47) „Urad za UI“ pomeni funkcijo Komisije, da prispeva k izvajanju, spremljanju in nadzoru sistemov UI in modelov UI za splošne namene ter upravljanju UI, določeno s Sklepom Komisije z dne 24. januarja 2024; v tej uredbi se sklicevanja na Urad za UI razumejo kot sklicevanja na Komisijo;

- (48) „pristojni nacionalni organ“ pomeni priglasitveni organ ali organ za nadzor trga; v zvezi s sistemi UI, ki so dani v uporabo ali jih uporabljajo institucije, agencije, uradi ali organi Unije, se sklicevanje na pristojne nacionalne organe ali organe za nadzor trga v tej uredbi razume kot sklicevanje na Evropskega nadzornika za varstvo podatkov;
- (49) „resen incident“ pomeni incident ali okvaro sistema UI, ki neposredno ali posredno povzroči naslednje:
- (a) smrt osebe ali resno škodo za zdravje osebe;
 - (b) resne in nepopravljive motnje pri upravljanju ali delovanju kritične infrastrukture;
 - (c) kršitev obveznosti iz prava Unije, namenjenih varstvu temeljnih pravic;
 - (d) resno škodo za premoženje ali okolje;
- (50) „osebni podatki“ pomeni osebne podatke, kakor so opredeljeni v členu 4, točka 1, Uredbe (EU) 2016/679;
- (51) „neosebni podatki“ pomeni podatke, ki niso osebni podatki, kakor so opredeljeni v členu 4, točka 1, Uredbe (EU) 2016/679;
- (52) „oblikovanje profilov“ pomeni oblikovanje profilov, kakor je opredeljeno v členu 4, točka 4, Uredbe (EU) 2016/679;

- (53) „načrt testiranja v realnih razmerah“ pomeni dokument, ki opisuje cilje, metodologijo, geografsko, populacijsko in časovno področje uporabe, spremljanje, organizacijo in izvajanje testiranja v realnih razmerah;
- (54) „načrt peskovnika“ pomeni dokument, o katerem se dogovorita sodelujoči ponudnik in pristojni organ in v katerem so opisani cilji, pogoji, časovni okvir, metodologija in zahteve za dejavnosti, ki se izvajajo v peskovniku;
- (55) „regulativni peskovnik za UI“ pomeni nadzorovan okvir, ki ga vzpostavi pristojni nacionalni organ in ki ponudnikom ali potencialnim ponudnikom sistemov UI omogoča, da na podlagi načrta peskovnika za omejen čas in pod regulativnim nadzorom razvijajo, učijo, potrdijo in testirajo, po potrebi v realnih razmerah, inovativen sistem UI;
- (56) „pismenost na področju UI“ pomeni spretnosti, znanje in razumevanje, ki ponudnikom, uvajalcem in zadevnim osebam, ob upoštevanju njihovih pravic in obveznosti v okviru te uredbe, omogočajo, da informirano uvajajo sisteme UI ter se hkrati zavedajo priložnosti in tveganj na področju UI in morebitne škode, ki jo ta lahko povzroči;
- (57) „testiranje v realnih razmerah“ pomeni začasno testiranje sistema UI za predvideni namen v realnih razmerah zunaj laboratorija ali drugače simuliranega okolja z namenom zbiranja zanesljivih in robustnih podatkov ter ugotavljanja in preverjanja skladnosti sistema UI z zahtevami iz te uredbe, pri čemer to ne šteje kot dajanje sistema UI na trg ali v uporabo v smislu te uredbe, če so izpolnjeni vsi pogoji iz člena 57 ali 60;

- (58) „udeleženec“ za namen testiranja v realnih razmerah pomeni fizično osebo, ki sodeluje pri testiranju v realnih razmerah;
- (59) „informirana privolitev“ pomeni svoboden, konkreten, nedvoumen in prostovoljen izraz pripravljenosti udeleženca, da sodeluje pri določenem testiranju v realnih razmerah, potem ko je bil seznanjen z vsemi vidiki testiranja, ki so pomembni za njegovo odločitev za sodelovanje.
- (60) „globoki ponaredek“ pomeni z UI ustvarjeno ali manipulirano slikovno, zvočno ali video vsebino, ki je podobna obstoječim osebam, predmetom, krajem, subjektom ali dogodkom in se uporabniku lažno zdi pristna ali resnična;
- (61) „močno razširjena kršitev“ pomeni vsako dejanje ali opustitev v nasprotju s pravom Unije o varstvu interesov posameznikov:
- (a) ki škoduje ali bi lahko škodovala kolektivnim interesom posameznikov, ki prebivajo v vsaj dveh državah članicah, ki nista država članica:
 - (i) iz katere izvira dejanje ali opustitev, oziroma v kateri je prišlo do dejanja ali opustitve;
 - (ii) v kateri se nahaja ali ima sedež zadevni ponudnik ali, kjer je ustrezno, njegov pooblaščen zastopnik ali
 - (iii) v kateri ima sedež uvajalec, kadar kršitev stori uvajalec;

- (b) ki je povzročila, povzroča ali bi lahko povzročila škodo kolektivnim interesom posameznikov in ki ima skupne značilnosti, med drugim enako nezakonito prakso ali kršitev istega interesa, stori pa jo isti operater sočasno v vsaj treh državah članicah;
- (62) „kritična infrastruktura“ pomeni kritično infrastrukturo, kakor je opredeljena v členu 2, točka 4, Direktive (EU) 2022/2557;
- (63) „model UI za splošne namene“ pomeni model UI, tudi kadar se takšen model UI uči z veliko količino podatkov z uporabo samonadzora v velikem obsegu, ki kaže znatno splošno uporabnost in je ne glede na to, kako je dan na trg, sposoben kompetentno opravljati širok nabor različnih nalog in ki ga je mogoče vključiti v različne sisteme ali aplikacije nižje v verigi, razen modelov UI, ki se uporabljajo za dejavnosti raziskav, razvoja ali izdelave prototipov, preden se dajo na trg;
- (64) „zmogljivosti z velikim vplivom“ pomeni zmogljivosti, ki so enake ali presegajo zmogljivosti, ki so zabeležene pri najbolj naprednih modelih UI za splošne namene;
- (65) „sistemsko tveganje“ pomeni tveganje, ki je specifično za zmogljivosti modelov UI za splošne namene z velikim vplivom in ima pomemben vpliv na trg Unije zaradi svojega dosega ali dejanskih ali razumno predvidljivih negativnih učinkov na javno zdravje, varnost, javno varnost, temeljne pravice ali družbo kot celoto, ki se lahko v širokem obsegu širijo po vsej verigi vrednosti;

- (66) „sistem UI za splošne namene“ pomeni sistem UI, ki temelji na modelu UI za splošne namene in lahko služi različnim namenom, tako za neposredno uporabo kot za integracijo v druge sisteme UI;
- (67) „operacija s plavajočo vejico“ (floating-point operation) pomeni vsako matematično operacijo ali nalogo, ki vključuje števila s plavajočo vejico, ki so podmnožica realnih števil, na računalnikih običajno predstavljenih s celim številom s fiksno natančnostjo, povečanim za celoštevilski eksponent s fiksno osnovo;
- (68) „ponudnik nižje v verigi“ pomeni ponudnika sistema UI, tudi sistema UI za splošne namene, ki vključuje model UI, ne glede na to, ali model ponuja sam in je vertikalno integriran ali pa ga ponuja drug subjekt na podlagi pogodbenih razmerij.

Člen 4

Pismenost na področju UI

Ponudniki in uvajalci sistemov UI sprejmejo ukrepe, da v najboljši možni meri zagotovijo zadostno raven pismenosti svojega osebja in tudi drugih oseb, ki se v njihovem imenu ukvarjajo z obratovanjem in uporabo sistemov UI, na področju UI, upoštevajoč njihovo tehnično znanje, izkušnje, izobrazbo in usposobljenost ter okolje, v katerem se bodo uporabljali sistemi UI, pa tudi osebe ali skupine oseb, v zvezi s katerimi se bodo uporabljali ti sistemi.

Poglavje II

Prepovedane prakse UI

Člen 5

Prepovedane prakse UI

1. Prepovedane so naslednje prakse UI:

- (a) dajanje na trg, dajanje v uporabo ali uporaba sistema UI, ki uporablja subliminalne tehnike, ki presegajo zavest osebe, ali namerno manipulativne ali zavajajoče tehnike, s ciljem ali učinkom bistvenega izkrivljanja vedenja osebe ali skupine oseb, tako da se znatno zmanjša njihova sposobnost, da sprejmejo informirano odločitev, zaradi česar sprejmejo odločitev, ki je sicer ne bi sprejeli, na način, ki tej osebi, drugi osebi ali skupini oseb povzroči znatno škodo ali za katerega obstaja razumna verjetnost, da bo povzročil znatno škodo;
- (b) dajanje na trg, dajanje v uporabo ali uporaba sistema UI, ki izkorišča katere koli šibke točke fizične osebe ali določene skupine oseb zaradi njihove starosti, invalidnosti ali posebnega socialnega ali ekonomskega položaja, s ciljem ali učinkom bistvenega izkrivljanja vedenja te osebe ali osebe iz te skupine na način, ki tej ali drugi osebi povzroči znatno škodo ali za katerega obstaja razumna verjetnost, da bo povzročil znatno škodo;

- (c) dajanje na trg, dajanje v uporabo ali uporaba sistemov UI za ocenjevanje ali razvrščanje fizičnih oseb ali skupin, ki jim pripadajo, v določenem časovnem obdobju na podlagi njihovega družbenega vedenja ali znanih, predpostavljenih ali predvidenih osebnih ali osebnostnih značilnosti, pri čemer število družbenih točk privede do ene ali obeh naslednjih možnosti:
- (i) škodljiva ali neugodna obravnava nekaterih fizičnih oseb ali skupin oseb v družbenih okoliščinah, ki niso povezane s konteksti, v katerih so bili podatki prvotno ustvarjeni ali zbrani;
 - (ii) škodljiva ali neugodna obravnava nekaterih fizičnih oseb ali skupin oseb, ki je neupravičena ali nesorazmerna z njihovim družbenim vedenjem ali resnostjo njihovega družbenega vedenja;
- (d) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistema UI za ocenjevanje tveganja v zvezi s fizičnimi osebami, da se oceni ali predvidi, kakšno je tveganje, da bo fizična oseba storila kaznivo dejanje, izključno na podlagi oblikovanja profila fizične osebe ali ocenjevanja njenih osebnostnih lastnosti in značilnosti; ta prepoved se ne uporablja za sisteme UI, ki se uporabljajo za podporo človeški oceni vpletenosti osebe v kriminalno dejavnost, ki že temelji na objektivnih in preverljivih dejstvih, neposredno povezanih s kriminalno dejavnostjo;
- (e) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov UI, ki z neciljnim odvzemom podob obraza z interneta ali s posnetkov kamer CCTV ustvarjajo ali širijo podatkovne zbirke za prepoznavanje obraza;

- (f) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov UI za sklepanje o čustvih fizične osebe na delovnem mestu in v izobraževalnih ustanovah, razen kadar je uporaba sistema UI namenjena uvedbi ali dajanju na trg iz zdravstvenih ali varnostnih razlogov;
- (g) dajanje na trg, dajanje v uporabo za ta posebni namen ali uporaba sistemov za biometrično kategorizacijo, ki posameznike razvrščajo na podlagi njihovih biometričnih podatkov, da bi prišli do sklepov ali ugotovitev glede njihove rase, političnega prepričanja, članstva v sindikatu, verskega ali filozofskega prepričanja, spolnega življenja ali spolne usmerjenosti; ta prepoved ne zajema označevanja ali filtriranja zakonito pridobljenih naborov biometričnih podatkov, kot so slike, na podlagi biometričnih podatkov ali kategorizacije biometričnih podatkov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj;
- (h) uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, razen če je taka uporaba nujno potrebna za enega od naslednjih ciljev:
 - (i) ciljno usmerjeno iskanje določenih žrtev ugrabitev, trgovine z ljudmi ali spolnega izkoriščanja ljudi ter iskanje pogrešanih oseb;
 - (ii) preprečitev konkretne, znatne in neposredne nevarnosti za življenje ali fizično varnost fizičnih oseb ali resnične in sedanje ali resnične in predvidljive grožnje terorističnega napada;

- (iii) lokalizacija ali identifikacija osebe, osumljene storitve kaznivega dejanja, za namen izvajanja kazenske preiskave ali pregona ali izvršitve kazenske sankcije za kazniva dejanja iz Priloge II, za katera je v zadevni državi članici predpisana zgornja meja zaporne kazni ali ukrepa, vezanega na odvzem prostosti, najmanj štiri leta.

Točka (h) prvega pododstavka ne posega v člen 9 Uredbe (EU) 2016/679 v zvezi z obdelavo biometričnih podatkov za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

- 2. Sistemi za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj za katerega koli od ciljev iz odstavka 1, prvi pododstavek, točka (h), se uporabljajo za namene iz navedene točke, samo da se potrdi identiteta točno določenega posameznika, pri čemer se upoštevajo naslednji elementi:
 - (a) narava razmer, ki povzročajo morebitno uporabo, zlasti resnost, verjetnost in obseg škode, ki bi bila povzročena, če se sistem ne bi uporabljal;
 - (b) posledice uporabe sistema za pravice in svoboščine vseh zadevnih oseb, zlasti resnost, verjetnost in obseg teh posledic.

Poleg tega mora biti uporaba sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj za katerega koli od ciljev iz odstavka 1, prvi pododstavek, točka (h), tega člena skladna s potrebnimi in sorazmernimi zaščitnimi ukrepi in pogoji v zvezi z uporabo po nacionalnem pravu, ki dovoljuje njihovo uporabo, zlasti kar zadeva časovne, geografske in osebne omejitve. Uporaba sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih se dovoli le, če je organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj opravil oceno učinka na temeljne pravice iz člena 27 in sistem registriral v podatkovni zbirki EU v skladu s členom 49. Vendar se lahko v ustrezno utemeljenih nujnih primerih uporaba takšnih sistemov začne brez registracije v podatkovni zbirki EU, če se takšna registracija zaključi brez nepotrebnega odlašanja.

3. Za namene odstavka 1, prvi pododstavek, točka (h), in odstavka 2 je za vsako uporabo sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj treba pridobiti predhodno dovoljenje sodnega organa ali neodvisnega upravnega organa, katerega odločitev je zavezujoča za državo članico, v kateri bo potekala uporaba, izdano na podlagi obrazložene zahteve in v skladu s podrobnimi pravili nacionalnega prava iz odstavka 5. Vendar se lahko v ustrezno utemeljenih nujnih primerih uporaba takšnega sistema začne brez dovoljenja, pod pogojem, da se takšno dovoljenje zahteva brez nepotrebnega odlašanja in najpozneje v 24 urah. Če se takšno dovoljenje zavrne, se njegova uporaba takoj ustavi, vsi podatki ter izhodni podatki in izsledki, ki izhajajo iz te uporabe, pa se takoj zavržejo in izbrišejo.

Pristojni sodni organ ali neodvisni upravni organ, katerega odločitev je zavezujoča, izda dovoljenje samo v primeru, kadar se na podlagi objektivnih dokazov ali jasnih navedb, ki so mu bili predloženi, prepriča, da je uporaba zadevnega sistema za biometrično identifikacijo na daljavo v realnem času potrebna in sorazmerna za doseganje enega od ciljev iz odstavka 1, prvi pododstavek, točka (h), kot je opredeljeno v zahtevi, in zlasti ostaja omejena na to, kar je nujno potrebno v zvezi z obdobjem ter geografskim in osebnim področjem uporabe. Pri odločanju o zahtevi ta organ upošteva elemente iz odstavka 2. Nobena odločitev, ki ima škodljiv pravni učinek na osebo, se ne sme sprejeti samo na podlagi izhodnih podatkov sistema za biometrično identifikacijo na daljavo v realnem času.

4. Brez poseganja v odstavek 3 je treba o vsaki uporabi sistema za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj uradno obvestiti ustrezni organ za nadzor trga in nacionalni organ za varstvo podatkov v skladu z nacionalnimi pravili iz odstavka 5. Obvestilo vsebuje vsaj informacije iz odstavka 6 in ne vključuje občutljivih operativnih podatkov.

5. Država članica se lahko odloči, da v okviru omejitev in pod pogoji iz odstavka 1, prvi pododstavek, točka (h), ter odstavkov 2 in 3 v celoti ali delno dovoli uporabo sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Zadevne države članice v svojem nacionalnem pravu določijo potrebna podrobna pravila v zvezi z vložitvijo zahteve za dovoljenja iz odstavka 3, izdajo, izvrševanjem in spremljanjem teh dovoljenj ter poročanjem v zvezi z njimi. V teh pravilih je tudi določeno, za katere od ciljev iz odstavka 1, prvi pododstavek, točka (h), med drugim tudi, za katera kazniva dejanja iz točke (h)(iii) navedenega odstavka, se lahko pristojnim organom dovoli uporaba teh sistemov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Države članice obvestijo Komisijo o teh pravilih najpozneje 30 dni po njihovem sprejetju. Države članice lahko v skladu s pravom Unije uvedejo strožje zakone o uporabi sistemov za biometrično identifikacijo na daljavo.
6. Nacionalni organi za nadzor trga in nacionalni organi za varstvo podatkov držav članic, ki so bili na podlagi odstavka 4 obveščeni o uporabi sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, Komisiji predložijo letna poročila o taki uporabi. V ta namen Komisija državam članicam ter nacionalnim organom za nadzor trga in varstvo podatkov zagotovi predlogo, ki vključuje informacije o številu odločitev, ki jih glede zahtevkov za dovoljenja v skladu z odstavkom 3 sprejmejo pristojni sodni organi ali neodvisni upravni organ, katerega odločitev je zavezujoča, in o njihovih rezultatih.

7. Komisija objavi letna poročila o uporabi sistemov za biometrično identifikacijo na daljavo v realnem času v javno dostopnih prostorih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj na podlagi zbirnih podatkov v državah članicah, ki temeljijo na letnih poročilih iz odstavka 6. Ta letna poročila ne vključujejo občutljivih operativnih podatkov o povezanih dejavnostih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.
8. Ta člen ne vpliva na prepovedi, ki se uporabljajo, kadar praksa UI krši drugo pravo Unije.

Poglavje III

Visokotvegani sistemi UI

ODDELEK 1

RAZVRSTITEV VISOKOTVEGANIH SISTEMOV UI

Člen 6

Pravila razvrstitve za visokotvegane sisteme UI

1. Ne glede na to, ali je sistem UI dan na trg ali v uporabo neodvisno od proizvodov iz točk (a) in (b), se ta sistem UI šteje za visokotvegani, kadar sta izpolnjena oba naslednja pogoja:
- (a) sistem UI je namenjen uporabi kot varnostna komponenta proizvoda ali pa je sam sistem UI proizvod, ki ga zajema harmonizacijska zakonodaja Unije iz Priloge I;

(b) za proizvod, katerega varnostna komponenta na podlagi točke (a) je sistem UI, ali za sistem UI, ki je sam proizvod, je treba opraviti ugotavljanje skladnosti s strani tretje osebe zaradi dajanja tega proizvoda na trg ali v uporabo na podlagi harmonizacijske zakonodaje Unije iz Priloge I.

2. Poleg visokotveganih sistemov UI iz odstavka 1 za visokotvegane sisteme UI štejejo tudi sistemi UI iz Priloge III.

3. Z odstopanjem od odstavka 2 sistem UI iz Priloge III ne šteje za visokotvegan, kadar ne predstavlja znatnega tveganja škode za zdravje, varnost ali temeljne pravice fizičnih oseb, tudi s tem, da ne vpliva bistveno na izid odločanja.

Prvi pododstavek se uporablja, kadar je izpolnjen kateri koli od naslednjih pogojev:

- (a) sistem UI naj bi opravljal omejeno postopkovno nalogo;
- (b) namen sistema UI je izboljšati rezultat predhodno zaključene človeške dejavnosti;
- (c) sistem UI je namenjen odkrivanju vzorcev odločanja ali odstopanj od predhodnih vzorcev odločanja in ni namenjen nadomeščanju ali vplivanju na predhodno dokončano človeško oceno brez ustreznega človeškega pregleda ali
- (d) sistem UI je namenjen izvedbi pripravljalne naloge za oceno, ki je pomembna za namene primerov uporabe iz Priloge III.

Ne glede na prvi pododstavek sistem UI iz Priloge III vedno šteje za visokotvegan, kadar izvaja oblikovanje profila fizičnih oseb.

4. Ponudnik, ki meni, da sistem UI iz Priloge III ne pomeni visokega tveganja, dokumentira svojo oceno, preden se ta sistem da na trg ali v uporabo. Za takega ponudnika velja obveznost registracije iz člena 49(2). Ponudnik na zahtevo pristojnih nacionalnih organov predloži dokumentacijo o oceni.
5. Komisija po posvetovanju z Evropskim odborom za umetno inteligenco (v nadaljnjem besedilu: Odbor) in najpozneje do ... [18 mesecev od datuma začetka veljavnosti te uredbe] zagotovi smernice, v katerih določi praktično izvajanje tega člena v skladu s členom 96, skupaj s celovitim seznamom praktičnih primerov uporabe visokotveganih sistemov UI in sistemov UI brez visokega tveganja.
6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da bi spremenila odstavek 3, drugi pododstavek, tega člena, s tem da bi k tam določenim pogojem dodala nove pogoje ali jih spremenila, kadar obstajajo konkretni in zanesljivi dokazi o obstoju sistemov UI, ki spadajo na področje uporabe Priloge III, vendar ne predstavljajo znatnega tveganja škode za zdravje, varnost ali temeljne pravice fizičnih oseb.

7. Komisija sprejme delegirane akte v skladu s členom 97, da bi spremenila kateri koli pogoj iz odstavka 3, drugi pododstavek, tega člena, s črtanjem katerih koli tam določenih pogojev, kadar obstajajo konkretni in zanesljivi dokazi, da je to potrebno za ohranjanje ravni varovanja zdravja, varnosti in temeljnih pravic iz te uredbe.
8. Nobena sprememba pogojev iz odstavka 3, drugi pododstavek, sprejeta v skladu z odstavkoma 6 in 7 tega člena, ne zmanjša splošne ravni varovanja zdravja, varnosti in temeljnih pravic iz te uredbe ter zagotovi skladnost z delegiranimi akti, sprejetimi na podlagi člena 7(1), ter upošteva tržni in tehnološki razvoj.

Člen 7

Spremembe Priloge III

1. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo Priloge III z dodajanjem primerov uporabe visokotveganih sistemov UI ali spreminjanjem njihove uporabe, kadar sta izpolnjena oba naslednja pogoja:
 - (a) sistemi UI so namenjeni uporabi na katerem koli področju iz Priloge III;
 - (b) sistemi UI predstavljajo tveganje škode za zdravje in varnost ali škodljivega vpliva na temeljne pravice in to tveganje je enakovredno ali večje od tveganja škode ali škodljivega vpliva visokotveganih sistemov UI, ki so že navedeni v Prilogi III.

2. Komisija pri ocenjevanju pogoja iz odstavka 1, točka (b), upošteva naslednja merila:
- (a) predvideni namen sistema UI;
 - (b) obseg, v katerem se sistem UI uporablja ali se bo verjetno uporabljal;
 - (c) naravo in količino podatkov, ki se obdelujejo in uporabljajo v sistemu UI, in zlasti to, ali se obdelujejo posebne vrste osebnih podatkov;
 - (d) obseg, v katerem sistem UI deluje samostojno, in možnost, da človek razveljavi odločitev ali priporočila, ki bi lahko povzročila morebitno škodo;
 - (e) obseg, v katerem je uporaba sistema UI že povzročila škodo za zdravje in varnost, negativno vplivala na temeljne pravice ali povzročila resno zaskrbljenost v zvezi z verjetnostjo take škode ali škodljivega vpliva, kot je razvidno na primer iz poročil ali dokumentiranih trditev, predloženih pristojnim nacionalnim organom, ali drugih poročil, kot je ustrezno;
 - (f) morebitni obseg take škode ali takega škodljivega vpliva, zlasti v smislu njune intenzivnosti in zmožnosti, da vplivata na več oseb ali nesorazmerno vplivata na določeno skupino ljudi;
 - (g) obseg, v katerem so potencialno oškodovane osebe ali osebe, ki bi lahko trpele zaradi škodljivega vpliva, odvisne od izida, ustvarjenega s sistemom UI, zlasti ker iz praktičnih ali pravnih razlogov ni mogoče razumno odstopiti od tega izida;

- (h) obseg, v katerem obstaja neravnovesje moči ali v katerem so potencialno oškodovane osebe ali osebe, ki bi lahko trpele zaradi škodljivega vpliva, v ranljivem položaju v odnosu do uvajalca sistema UI, zlasti zaradi statusa, avtoritete, znanja, ekonomskih ali socialnih okoliščin ali starosti;
- (i) obseg, v katerem je rezultat, ki vključuje sistem UI, zlahka popravljiv ali izničljiv, ob upoštevanju razpoložljivih tehničnih rešitev za njegovo popravljanje ali izničenje, pri čemer rezultati, ki škodljivo vplivajo na zdravje, varnost ali temeljne pravice, ne štejejo za zlahka popravljive ali izničljive;
- (j) razsežnost in verjetnost, da bo uvedba sistema UI koristila posameznikom, skupinam ali družbi na splošno, vključno z možnimi izboljšavami glede varnosti proizvodov;
- (k) obseg, v katerem so v obstoječem pravu Unije določeni:
 - (i) učinkoviti ukrepi sodnega varstva v zvezi s tveganji, ki jih predstavlja sistem UI, razen odškodninskih zahtevkov;
 - (ii) učinkoviti ukrepi za preprečevanje ali bistveno zmanjšanje teh tveganj.

3. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo seznama iz Priloge III z umikom visokotveganih sistemov UI, kadar sta izpolnjena oba naslednja pogoja:
- (a) zadevni visokotvegani sistem UI ob upoštevanju meril iz odstavka 2 ne predstavlja več večjih tveganj za temeljne pravice, zdravje ali varnost;
 - (b) črtanje ne zmanjšuje splošne ravni varovanja zdravja, varnosti in temeljnih pravic na podlagi prava Unije.

ODDELEK 2

ZAHTEVE ZA VISOKOTVEGANE SISTEME UI

Člen 8

Izpolnjevanje zahtev

1. Visokotvegani sistemi UI izpolnjujejo zahteve iz tega oddelka, pri čemer se upoštevajo njihovi predvideni namen ter splošno priznani najsodobnejši dosežki na področju UI in tehnologij, povezanih z UI. Pri zagotavljanju skladnosti z navedenimi zahtevami se upošteva sistem za obvladovanje tveganja iz člena 9.

2. Kadar proizvod vključuje sistem UI, za katerega se uporabljajo zahteve iz te uredbe in zahteve harmonizacijske zakonodaje Unije iz Priloge I, oddelek A, so ponudniki odgovorni za zagotavljanje popolne usklajenosti njihovega proizvoda z vsemi veljavnimi zahtevami iz veljavne harmonizacijske zakonodaje Unije. Ponudniki imajo pri zagotavljanju skladnosti visokotveganih sistemov UI iz odstavka 1 z zahtevami iz tega oddelka ter za zagotovitev skladnosti, preprečevanje podvajanja in zmanjšanje dodatnih bremen možnost, da po potrebi vključijo potrebne postopke testiranja in poročanja, informacije in dokumentacijo, ki jih predložijo v zvezi s svojim proizvodom, v dokumentacijo in postopke, ki že obstajajo in se zahtevajo na podlagi harmonizacijske zakonodaje Unije iz Priloge I, oddelek A.

Člen 9

Sistem za obvladovanje tveganja

1. V zvezi z visokotveganimi sistemi UI se vzpostavi, izvaja, dokumentira in vzdržuje sistem za obvladovanje tveganja.
2. Sistem za obvladovanje tveganja pomeni neprekinjen in ponavljajoč se proces, ki se načrtuje in izvaja v celotnem življenjskem ciklu visokotveganega sistema UI in ga je treba redno sistematično pregledovati in posodabljati. Vključuje naslednje korake:
 - (a) opredelitev in analizo znanih in razumno predvidljivih tveganj, ki jih lahko visokotvegani sistem UI pomeni za zdravje, varnost ali temeljne pravice, kadar se uporablja v skladu s predvidenim namenom;

- (b) oceno in ovrednotenje tveganj, ki se lahko pojavijo pri uporabi visokotveganega sistema UI v skladu s predvidenim namenom in v razmerah razumno predvidljive napačne uporabe;
 - (c) ovrednotenje drugih morebitnih tveganj na podlagi analize podatkov, zbranih iz sistema spremljanja po dajanju na trg iz člena 72;
 - (d) sprejetje ustreznih in ciljno usmerjenih ukrepov za obvladovanje tveganja, namenjenih obravnavanju tveganj, opredeljenih na podlagi točke (a).
3. Tveganja iz tega člena se nanašajo samo na tista, ki jih je mogoče razumno zmanjšati ali odpraviti z razvojem ali zasnovo visokotveganega sistema UI ali z zagotovitvijo ustreznih tehničnih informacij.
4. Pri ukrepih za obvladovanje tveganja iz odstavka 2, točka (d), se ustrezno upoštevajo učinki in morebitna interakcija, ki izhajajo iz skupne uporabe zahtev iz tega oddelka 2, da bi učinkoviteje in čim bolj zmanjšali tveganja in hkrati dosegli ustrezno ravnovesje pri izvajanju ukrepov za izpolnjevanje teh zahtev.
5. Ukrepi za obvladovanje tveganja iz odstavka 2, točka (d), so taki, da zadevno preostalo tveganje, povezano z vsako posamezno nevarnostjo, in celotno preostalo tveganje visokotveganih sistemov UI štejeta za sprejemljiva.

Pri določanju najustrežnejših ukrepov za obvladovanje tveganja se zagotovi naslednje:

- (a) odpravljanje ali zmanjševanje tveganj ugotovljenih in ocenjenih na podlagi odstavka 2, kolikor je to tehnično izvedljivo z ustrezno zasnovo in razvojem visokotveganega sistema UI;
- (b) po potrebi izvajanje ustreznih ukrepov za zmanjšanje in nadzor tveganj, ki jih ni mogoče odpraviti;
- (c) zagotavljanje zahtevanih informacij na podlagi člena 13 in po potrebi usposabljanje uvajalcev.

Da bi odpravili ali zmanjšali tveganja, povezana z uporabo visokotveganega sistema UI, se ustrezno upoštevajo tehnično znanje, izkušnje, izobraževanje, usposabljanje, ki ga lahko pričakuje uvajalec, in predvideni okvir, v katerem naj bi se sistem uporabljal.

- 6. Visokotvegani sistemi UI se testirajo, da se določijo najustrežnejši in ciljno usmerjeni ukrepi za obvladovanje tveganja. S testiranjem se zagotovi, da visokotvegani sistemi UI dosledno delujejo za predvideni namen in so skladni z zahtevami iz tega oddelka.
- 7. Postopki testiranja lahko vključujejo testiranje v realnih razmerah v skladu s členom 60.

8. Testiranje visokotveganih sistemov UI se po potrebi izvaja kadar koli med celotnim postopkom razvoja in v vsakem primeru pred njihovim dajanjem na trg ali v uporabo. Testiranje se opravi na podlagi predhodno opredeljenih metrik in verjetnostnih pragov, ki ustrezajo predvidenemu namenu visokotveganega sistema UI.
9. Ponudniki pri izvajanju sistema za obvladovanje tveganja iz odstavkov 1 do 7 preučijo, ali je verjetno, da bo visokotvegani sistem UI glede na predvideni namen negativno vplival na osebe, mlajše od 18 let, in po potrebi na druge ranljive skupine.
10. Pri ponudnikih visokotveganih sistemov UI, za katere veljajo zahteve v zvezi z notranjimi procesi za obvladovanje tveganj v skladu z drugimi ustreznimi določbami prava Unije, so lahko vidiki, opisani v odstavkih 1 do 9, del postopkov za obvladovanje tveganj, vzpostavljenih na podlagi navedenega prava, ali so v kombinaciji s temi postopki.

Člen 10

Podatki in upravljanje podatkov

1. Visokotvegani sistemi UI, ki uporabljajo tehnike, ki vključujejo učenje modelov UI s podatki, se razvijejo na podlagi naborov učnih, validacijskih in testnih podatkov, ki izpolnjujejo merila kakovosti iz odstavkov 2 do 5, kadar se uporabljajo ti nabori podatkov.

2. Za nabore učnih, validacijskih in testnih podatkov veljajo prakse ravnanja s podatki in upravljanja podatkov, ki so primerne za predvideni namen visokotveganega sistema UI. Te prakse se nanašajo zlasti na:
- (a) ustrezne izbire zasnov;
 - (b) postopke zbiranja podatkov in njihov izvor ter v primeru osebnih podatkov prvotni namen zbiranja podatkov;
 - (c) ustrezne postopke obdelave za pripravo podatkov, kot so dodajanje opomb, označevanje, čiščenje, posodabljanje, obogatitev in združevanje;
 - (d) oblikovanje predpostavk, zlasti v zvezi z informacijami, ki naj bi jih podatki merili in predstavljali;
 - (e) oceno razpoložljivosti, količine in primernosti potrebnih naborov podatkov;
 - (f) preučitev morebitnih pristranskosti, ki bi lahko vplivale na zdravje in varnost oseb, negativno vplivale na temeljne pravice ali privedle do diskriminacije, ki je na podlagi prava Unije prepovedana, zlasti kadar izhodni podatki vplivajo na vhodne podatke za prihodnje operacije;
 - (g) ustrezne ukrepe za odkrivanje, preprečevanje in zmanjševanje morebitnih pristranskosti, opredeljenih v skladu s točko (f);
 - (h) prepoznavanje ustreznih vrzeli ali pomanjkljivosti v podatkih, ki preprečujejo skladnost s to uredbo, ter način za odpravljanje teh vrzeli in pomanjkljivosti.

3. Nabori učnih, validacijskih in testnih podatkov so ustrezni, dovolj reprezentativni in v največji možni meri brez napak in popolni glede na predvideni namen. Imeti morajo tudi ustrezne statistične lastnosti, po potrebi tudi v zvezi z osebami ali skupinami oseb, v zvezi s katerimi naj bi se uporabljal visokotvegani sistem UI. Te značilnosti naborov podatkov se lahko izpolnijo na ravni posameznih naborov podatkov ali na ravni njihovih kombinacij.
4. Nabori podatkov v obsegu, ki se zahteva glede na njihov predvideni namen, upoštevajo značilnosti ali elemente, ki so značilni za posebno geografsko, kontekstualno, vedenjsko ali funkcionalno okolje, v katerem naj bi se visokotvegani sistem UI uporabljal.
5. Če je nujno potrebno za namene zagotavljanja odkrivanja in popravljanja pristranskosti v zvezi z visokotveganimi sistemi UI v skladu z odstavkom 2, točki (f) in (g), tega člena, lahko ponudniki takih sistemov izjemoma obdelujejo posebne vrste osebnih podatkov, ob upoštevanju ustreznih zaščitnih ukrepov za temeljne pravice in svoboščine fizičnih oseb. Poleg določb iz uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktive (EU) 2016/680 morajo biti za tako obdelavo izpolnjeni vsi naslednji pogoji:
 - (a) odkrivanja in popravljanja pristranskosti ni mogoče učinkovito doseči z obdelavo drugih podatkov, vključno s sintetičnimi ali anonimiziranimi podatki;

- (b) za posebne vrste osebnih podatkov veljajo tehnične omejitve glede ponovne uporabe osebnih podatkov ter najsodobnejši ukrepi za varnost in ohranjanje zasebnosti, vključno s psevdonimizacijo;
- (c) za posebne kategorije osebnih podatkov veljajo ukrepi, s katerimi se zagotavlja, da so osebni podatki, ki se obdelujejo, zaščiteni, ob upoštevanju ustreznih zaščitnih ukrepov, vključno s strogim nadzorom in dokumentiranjem dostopa, da se prepreči napačna uporaba in zagotovi, da imajo dostop do teh osebnih podatkov samo pooblaščen osebe z ustreznimi obveznostmi glede zaupnosti;
- (d) posebne kategorije osebnih podatkov ne smejo biti posredovani, preneseni ali drugače dostopni drugim strankam;
- (e) posebne kategorije osebnih podatkov se izbrišejo, ko je pristranskost odpravljena ali ko se izteče obdobje njihove hrambe, odvisno od tega, kaj nastopi prej;
- (f) evidence dejavnosti obdelave na podlagi uredb (EU) 2016/679 in (EU) 2018/1725 ter Direktivo (EU) 2016/680 vključujejo razloge, zakaj je bila obdelava posebnih kategorij osebnih podatkov nujno potrebna za odkrivanje in odpravo pristranskosti ter zakaj tega cilja ni bilo mogoče doseči z obdelavo drugih podatkov.

6. Za razvoj visokotveganih sistemov UI, ki ne uporabljajo tehnik, ki vključujejo učenje modelov s podatki, se odstavki 2 do 5 uporabljajo le za nabore testnih podatkov.

Člen 11
Tehnična dokumentacija

1. Tehnična dokumentacija visokotveganega sistema UI se pripravi pred dajanjem sistema na trg ali v uporabo in se posodablja.

Tehnična dokumentacija se pripravi tako, da izkazuje, da je visokotvegani sistem UI skladen z zahtevami iz tega oddelka, ter pristojnim nacionalnim organom in priglašnim organom jasno in celovito zagotavlja potrebne informacije za ugotavljanje skladnosti sistema UI z navedenimi zahtevami. Vsebovati mora vsaj elemente iz Priloge IV. MSP, vključno z zagonskimi podjetji, lahko elemente tehnične dokumentacije iz Priloge IV predložijo na poenostavljen način. V ta namen Komisija pripravi poenostavljen obrazec tehnične dokumentacije, namenjen potrebam malih in mikro podjetij. Kadar se MSP, vključno z zagonskim podjetjem, odloči, da bo informacije, zahtevane v Prilogi IV, zagotovilo na poenostavljen način, uporabi obrazec iz tega odstavka. Priglašeni organi sprejmejo obrazec za namene ugotavljanja skladnosti.

2. Kadar je visokotvegani sistem UI, povezan s proizvodom, za katerega se uporablja harmonizacijska zakonodaja Unije iz Priloge I, oddelek A, dan na trg ali v uporabo, se pripravi enoten sklop tehnične dokumentacije, ki vsebuje vse informacije iz odstavka 1 in informacije, zahtevane v navedenih pravnih aktih.

3. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo Priloge IV, kadar je to potrebno za zagotovitev, da tehnična dokumentacija glede na tehnični napredek zagotavlja vse potrebne informacije za ugotavljanje skladnosti sistema z zahtevami iz tega oddelka.

Člen 12

Vodenje evidenc

1. Visokotvegani sistemi UI morajo tehnično omogočati samodejno beleženje dogodkov (v nadaljnjem besedilu: dnevniki) v življenjski dobi sistema.
2. Da bi zagotovili raven sledljivosti delovanja visokotveganega sistema UI, ki ustreza predvidenemu namenu sistema, morajo zmogljivosti vodenja dnevnikov omogočati beleženje dogodkov, pomembnih za:
 - (a) prepoznavanje situacij, ki lahko povzročijo, da bi visokotvegani sistem UI predstavljal tveganje v smislu člena 79(1), ali povzročijo bistvene spremembe;
 - (b) olajšanje spremljanja po dajanju na trg iz člena 72 ter
 - (c) spremljanje delovanja visokotveganega sistema UI iz člena 26(5).
3. Za visokotvegane sisteme UI iz Priloge III, točka 1(a), zmogljivosti vodenja dnevnikov zagotavljajo vsaj:
 - (a) evidentiranje obdobja vsake uporabe sistema (datum in čas začetka ter datum in čas konca vsake uporabe);

- (b) referenčno podatkovno zbirko, s katero je sistem preveril vhodne podatke;
- (c) vhodne podatke, za katere je bilo pri iskanju najdeno ujemanje;
- (d) identifikacijo fizičnih oseb, ki sodelujejo pri preverjanju rezultatov, iz člena 14(5).

Člen 13

Preglednost in zagotavljanje informacij uvajalcem

1. Visokotvegani sistemi UI morajo biti zasnovani in razviti tako, da je njihovo delovanje dovolj pregledno, da lahko uvajalci razlagajo izhodne podatke sistema in jih ustrezno uporabijo. Treba je zagotoviti ustrezno vrsto in stopnjo preglednosti, da se doseže skladnost z ustreznimi obveznostmi ponudnika in uvajalca iz oddelka 3.
2. Visokotveganim sistemom UI morajo biti priložena navodila za uporabo v ustrezni digitalni obliki ali kako drugače, ki vključujejo jedrnate, popolne, pravilne in jasne informacije, ki so pomembne, dostopne in razumljive uvajalcem.
3. Navodila za uporabo vsebujejo vsaj naslednje informacije:
 - (a) istovetnost in kontaktne podatke ponudnika in po potrebi njegovega pooblaščenega zastopnika, kadar obstaja;

- (b) značilnosti, zmogljivosti in omejitve zmogljivosti visokotveganega sistema UI, ki vključujejo:
- (i) njegov predvideni namen;
 - (ii) raven točnosti, vključno s pripadajočimi metrikami, robustnosti in kibernetске varnosti iz člena 15, na podlagi katere je bil visokotvegani sistem UI testiran in potrjen ter ki se lahko pričakuje, pa tudi vse znane in predvidljive okoliščine, ki bi lahko vplivale na to pričakovano raven točnosti, robustnosti in kibernetске varnosti;
 - (iii) vse znane ali predvidljive okoliščine, povezane z uporabo visokotveganega sistema UI v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, ki lahko povzročijo tveganja za zdravje in varnost ali temeljne pravice iz člena 9(2);
 - (iv) po potrebi tehnične zmogljivosti in značilnosti visokotveganega sistema UI za zagotavljanje informacij, ki so pomembne za pojasnitev njegovih izhodnih podatkov;
 - (v) če je primerno, njegova zmogljivost v zvezi z določenimi osebami ali skupinami oseb, na katerih naj bi se sistem uporabljal;
 - (vi) če je primerno, specifikacije za vhodne podatke ali katere koli druge ustrezne informacije v zvezi z uporabljenimi nabori učnih, validacijskih in testnih podatkov, ob upoštevanju predvidenega namena visokotveganega sistema UI;

- (vii) po potrebi informacije, da lahko uvajalci razlagajo izhodne podatke visokotveganega sistema UI in jih ustrezno uporabljajo;
- (c) morebitne spremembe visokotveganega sistema UI in njegove zmogljivosti, ki jih je ponudnik vnaprej določil ob začetnem ugotavljanju skladnosti;
- (d) ukrepe za človeški nadzor iz člena 14, vključno z vzpostavljenimi tehničnimi ukrepi, ki uvajalcem olajšajo razlago izhodnih podatkov visokotveganih sistemov UI;
- (e) potrebne računalniške in strojnoopremne vire, življenjsko dobo visokotveganega sistema UI ter vse potrebne vzdrževalne in oskrbovalne ukrepe, vključno z njihovo pogostostjo, za zagotovitev pravilnega delovanja tega sistema UI, tudi kar zadeva posodobitve programske opreme;
- (f) po potrebi opis mehanizmov v visokotveganem sistemu UI, na podlagi katerega lahko uvajalci pravilno zbirajo, hranijo in razlagajo dnevnik v skladu s členom 12.

Člen 14

Človeški nadzor

1. Visokotvegani sistemi UI morajo biti zasnovani in razviti tako, da jih lahko fizične osebe v obdobju njihove uporabe učinkovito nadzorujejo, tudi z ustreznimi vmesniškimi orodji človek-stroj.

2. Namen človeškega nadzora je preprečiti ali čim bolj zmanjšati tveganja za zdravje, varnost ali temeljne pravice, ki se lahko pojavijo pri uporabi visokotveganega sistema UI v skladu s predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, zlasti kadar taka tveganja niso odpravljena kljub uporabi drugih zahtev iz tega oddelka.
3. Nadzorni ukrepi morajo biti sorazmerni s tveganji, stopnjo samostojnosti in kontekstom uporabe visokotveganega sistema UI in se zagotavljajo z eno ali obema naslednjima vrstama ukrepov:
 - (a) ukrepi, določeni in vgrajeni, če je to tehnično izvedljivo, v visokotvegani sistem UI s strani ponudnika, preden je sistem dan na trg ali v uporabo;
 - (b) ukrepi, ki jih ponudnik določi pred dajanjem visokotveganega sistema UI na trg ali v uporabo in so primerni za izvedbo s strani uvajalca.
4. Za namene izvajanja odstavkov 1, 2 in 3 se visokotvegani sistem UI uvajalcu zagotovi tako, da fizične osebe, ki jim je dodeljen človeški nadzor, če je to primerno in sorazmerno:
 - (a) pravilno razumejo ustrezne zmogljivosti in omejitve visokotveganega sistema UI ter ustrezno spremljajo njegovo delovanje, tudi za odkrivanje in obravnavanje nepravilnosti, motenj in nepričakovane zmogljivosti;

- (b) se zavedajo morebitne težnje po samodejnem zanašanju ali prevelikem zanašanju na izhodne podatke visokotveganega sistema UI (pristranskost zaradi avtomatizacije), zlasti pri visokotveganih sistemih UI, ki se uporabljajo za zagotavljanje informacij ali priporočil za odločitve, ki jih sprejemajo fizične osebe;
- (c) pravilno razlagajo izhodne podatke visokotveganega sistema UI, zlasti na primer ob upoštevanju razpoložljivih orodij in metod za razlago;
- (d) se v specifičnih situacijah odločijo, da visokotveganega sistema UI ne bodo uporabile ali bodo kako drugače zanemarile, ovrgle ali izničile izhodne podatke visokotveganega sistema UI;
- (e) posegajo v delovanje visokotveganega sistema UI ali ga prekinajo s tipko „stop“ ali podobnim postopkom, ki omogoča varno zaustavitev sistema.

5. Za visokotvegane sisteme UI iz Priloge III, točka 1(a), morajo biti ukrepi iz odstavka 3 takšni, da zagotavljajo, da uvajalec poleg tega ne izvede nobenega dejanja ali ne sprejme nobenega ukrepa ali odločitve na podlagi identifikacije, ki izhaja iz sistema, razen če to ločeno preverita in potrdita vsaj dve fizični osebi z ustreznimi kompetencami, usposobljenostjo in pooblastili.

Zahteva o ločeni preverbi s strani vsaj dveh fizičnih oseb se ne uporablja za visokotvegane sisteme UI, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, nadzora meje ali azila, v primerih, ko je v skladu s pravom Unije in nacionalnim pravom uporaba te zahteve nesorazmerna.

Člen 15

Točnost, robustnost in kibernetska varnost

1. Visokotvegani sistemi UI morajo biti zasnovani in razviti tako, da dosegajo ustrezno raven točnosti, robustnosti in kibernetske varnosti ter v teh vidikih v vsem svojem življenjskem ciklu delujejo dosledno.
2. Za obravnavo tehničnih vidikov merjenja ustreznih ravni točnosti in robustnosti iz odstavka 1 ter vseh drugih ustreznih metrike učinkovitosti Komisija v sodelovanju z ustreznimi deležniki in organizacijami, kot so meroslovni organi in organi za primerjalno analizo, po potrebi spodbuja razvoj referenčnih vrednosti in metodologij merjenja.
3. Ravni točnosti in ustrezne metrike točnosti visokotveganih sistemov UI se navedejo v priloženih navodilih za uporabo.
4. Visokotvegani sistemi UI morajo biti čim bolj odporni na napake, okvare ali neskladnosti, ki se lahko pojavijo v sistemu ali okolju, v katerem sistem deluje, zlasti zaradi njihove interakcije s fizičnimi osebami ali drugimi sistemi. V zvezi s tem se sprejmejo tehnični in organizacijski ukrepi.

Robustnost visokotveganih sistemov UI se lahko doseže s tehničnimi redundantnimi rešitvami, ki lahko vključujejo rezervne načrte ali načrte varne odpovedi.

Visokotvegane sisteme UI, ki se po dajanju na trg ali v uporabo še naprej učijo, je treba razviti tako, da se odpravi ali v največji možni meri zmanjša tveganje morebitnih pristranskih izhodnih podatkov, ki bi vplivali na vhodne podatke za prihodnje operacije (povratne zanke), in zagotovi, da se vse take povratne zanke ustrezno obravnavajo z ustreznimi ukrepi za zmanjšanje tveganj.

5. Visokotvegani sistemi UI morajo biti odporni na poskuse nepooblaščenih tretjih oseb, da z izkoriščanjem šibkih točk sistema spremenijo njihovo uporabo, izhodne podatke ali zmogljivost.

Tehnične rešitve, namenjene zagotavljanju kibernetске varnosti visokotveganih sistemov UI, morajo ustrezati zadevnim okoliščinam in tveganjem.

Tehnične rešitve za odpravljanje šibkih točk, značilnih za UI, po potrebi vključujejo ukrepe za preprečevanje, odkrivanje, odzivanje, reševanje in nadzor v zvezi z napadi, ki poskušajo manipulirati z naborom učnih podatkov (zastrupitev podatkov) ali prednaučenimi komponentami, uporabljenimi pri učenju (zastrupitev modelov), v zvezi z vhodnimi podatki, katerih namen je povzročiti napako modela UI (nasprotovalni primer ali izogibanje modelov), napadi na zaupnost ali pomanjkljivostmi modela.

ODDELEK 3
OBVEZNOSTI PONUDNIKOV IN UVAJALCEV VISOKOTVEGANIH
SISTEMOV UI

Člen 16

Obveznosti ponudnikov visokotveganih sistemov UI

Ponudniki visokotveganih sistemov UI:

- (a) zagotovijo, da so njihovi visokotvegani sistemi UI skladni z zahtevami iz oddelka 2;
- (b) na visokotvegane sistem UI ali, kadar to ni mogoče, na embalaži ali spremni dokumentaciji, kot je ustrezno, navedejo svoje ime, registrirano trgovsko ime ali registrirano znamko, in naslov, na katerem so dosegljivi;
- (c) imajo vzpostavljen sistem upravljanja kakovosti, skladen s členom 17;
- (d) hranijo dokumentacijo iz člena 18;
- (e) kadar je to pod njihovim nadzorom, hranijo dnevnike, ki jih samodejno ustvarijo njihovi visokotvegani sistemi UI, kot je navedeno v členu 19;
- (f) zagotovijo, da visokotvegani sistem UI pred dajanjem na trg ali v uporabo opravi ustrezen postopek ugotavljanja skladnosti iz člena 43;

- (g) pripravijo EU izjavo o skladnosti v skladu s členom 47;
- (h) na visokotvegani sistem UI ali, kadar to ni mogoče, na njegovo embalažo ali priloženo dokumentacijo, namestijo oznako CE v skladu s členom 48, da označijo skladnost s to uredbo;
- (i) izpolnjujejo obveznosti registracije iz člena 49(1);
- (j) sprejmejo potrebne korektivne ukrepe in zagotovijo informacije v skladu s členom 20;
- (k) na obrazloženo zahtevo pristojnega nacionalnega organa dokažejo skladnost visokotveganega sistema UI z zahtevami iz oddelka 2;
- (l) zagotovijo, da visokotvegani sistem UI izpolnjuje zahteve glede dostopnosti v skladu z direktivama (EU) 2016/2102 in (EU) 2019/882.

Člen 17

Sistem upravljanja kakovosti

1. Ponudniki visokotveganih sistemov UI vzpostavijo sistem upravljanja kakovosti, ki zagotavlja skladnost s to uredbo. Ta sistem se sistematično in urejeno dokumentira v obliki pisnih politik, postopkov in navodil ter vključuje vsaj naslednje vidike:
 - (a) strategijo za skladnost z zakonodajo, tudi skladnost s postopki za ugotavljanje skladnosti in postopki za upravljanje sprememb visokotveganega sistema UI;

- (b) tehnike, postopke in sistematične ukrepe, ki se uporabljajo za razvoj, nadzor kakovosti in zagotavljanje kakovosti visokotveganega sistema UI;
- (c) tehnike, postopke in sistematične ukrepe, ki se uporabljajo za razvoj, nadzor kakovosti in zagotavljanje kakovosti visokotveganega sistema UI;
- (d) postopke pregledovanja, testiranja in validacije, ki se izvedejo pred razvojem visokotveganega sistema UI, med njim in po njem, ter pogostost njihovega izvajanja;
- (e) tehnične specifikacije, vključno s standardi, ki jih je treba uporabiti, in, kadar se ustrezni harmonizirani standardi ne uporabljajo v celoti ali ne zajemajo vseh ustreznih zahtev iz oddelka 2, sredstva, ki se uporabijo za zagotovitev, da visokotvegani sistem UI izpolnjuje navedene zahteve;
- (f) sisteme in postopke za ravnanje s podatki, vključno s pridobivanjem podatkov, zbiranjem podatkov, analizo podatkov, označevanjem podatkov, shranjevanjem podatkov, filtriranjem podatkov, podatkovnim rudarjenjem, združevanjem podatkov, hrambo podatkov ter vsemi drugimi postopki v zvezi s podatki, ki se izvajajo pred dajanjem visokotveganih sistemov UI na trg ali v uporabo in za namen dajanja na trg ali v uporabo;
- (g) sistem za obvladovanje tveganj iz člena 9;
- (h) vzpostavitev, izvajanje in vzdrževanje sistema spremljanja po dajanju na trg v skladu s členom 72;

- (i) postopke v zvezi s poročanjem o resnih incidentih v skladu s členom 73;
 - (j) vodenje komunikacije s pristojnimi nacionalnimi organi, drugimi ustreznimi organi, tudi s tistimi, ki zagotavljajo ali podpirajo dostop do podatkov, priglašeni organi, drugimi operaterji, strankami ali drugimi zainteresiranimi stranmi;
 - (k) sisteme in postopke za vodenje evidenc vse ustrezne dokumentacije in informacij;
 - (l) upravljanje virov, vključno z ukrepi, povezanimi z zanesljivostjo oskrbe;
 - (m) okvir odgovornosti, ki določa odgovornosti vodstva in drugega osebja v zvezi z vsemi vidiki iz tega odstavka.
2. Izvajanje vidikov iz odstavka 1 je sorazmerno z velikostjo organizacije ponudnika. V vsakem primeru pa ponudniki spoštujejo stopnjo strogosti in raven zaščite, ki se zahtevata za skladnost njihovih visokotveganih sistemov UI s to uredbo.
3. Ponudniki visokotveganih sistemov UI, za katere veljajo obveznosti v zvezi s sistemi upravljanja kakovosti ali enakovredno funkcijo na podlagi ustreznega sektorskega prava Unije, lahko vključijo vidike, navedene v odstavku 1, kot del sistemov upravljanja kakovosti, vzpostavljenih na podlagi navedenega prava.

4. Za ponudnike, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, se šteje, da je obveznost vzpostavitve sistema vodenja kakovosti z izjemo odstavka 1, točke (g), (h) in (i) tega člena, izpolnjena z upoštevanjem pravil o ureditvah ali postopkih notranjega upravljanja na podlagi ustreznega prava Unije o finančnih storitvah. V ta namen se upoštevajo vsi harmonizirani standardi iz člena 40.

Člen 18

Vodenje dokumentacije

1. Ponudnik še deset let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo, za pristojni nacionalni organ hrani:
- (a) tehnično dokumentacijo iz člena 11;
 - (b) dokumentacijo v zvezi s sistemom upravljanja kakovosti iz člena 17;
 - (c) dokumentacijo o spremembah, ki so jih odobrili priglašeni organi, kadar je primerno;
 - (d) odločitve in druge dokumente, ki so jih izdali priglašeni organi, kadar je primerno;
 - (e) EU izjavo o skladnosti iz člena 47.

2. Vsaka država članica določi pogoje, pod katerimi je dokumentacija iz odstavka 1 na voljo pristojnim nacionalnim organom v obdobju iz navedenega odstavka v primerih, ko gre ponudnik ali njegov pooblaščen zastopnik, ki ima sedež na njenem ozemlju, v stečaj ali preneha opravljati svojo dejavnost pred koncem tega obdobja.
3. Ponudniki, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, vodijo tehnično dokumentacijo kot del dokumentacije, ki se hrani na podlagi ustreznega prava Unije o finančnih storitvah.

Člen 19

Samodejno ustvarjeni dnevniki

1. Ponudniki visokotveganih sistemov UI vodijo dnevnike iz člena 12(1), ki jih samodejno ustvarijo njihovi visokotvegani sistemi UI, če so ti dnevniki pod njihovim nadzorom. Brez poseganja v pravo Unije ali nacionalno pravo, ki se uporablja, se dnevniki hranijo za obdobje, ki ustreza predvidenemu namenu visokotvegane sistema UI, in sicer najmanj šest mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvu osebnih podatkov, določeno drugače.
2. Ponudniki, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, vodijo dnevnike, ki jih samodejno ustvarijo njihovi visokotvegani sistemi UI, kot del dokumentacije, ki se hrani na podlagi ustreznega prava Unije o finančnih storitvah.

Člen 20

Korektivni ukrepi in dolžnost obveščanja

1. Ponudniki visokotveganih sistemov UI, ki menijo ali utemeljeno domnevajo, da visokotvegani sistem UI, ki so ga dali na trg ali v uporabo, ni v skladu s to uredbo, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost sistema ali pa ga po potrebi umaknejo, onemogočijo ali prekličejo. O tem obvestijo distributerje zadevnega visokotveganega sistema UI ter, kadar je primerno, uvajalce, pooblaščenega zastopnika in uvoznike.
2. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1) in se ponudnik seznani s tem tveganjem, nemudoma razišče vzroke, po potrebi v sodelovanju z uvajalcem, ki poroča, ter obvesti organe za nadzor trga, pristojne za zadevni visokotvegani sistem UI, in po potrebi priglasi organ, ki je izdal certifikat za visokotvegani sistem UI v skladu s členom 44, zlasti o naravi neskladnosti in vseh ustreznih sprejetih korektivnih ukrepih.

Člen 21

Sodelovanje s pristojnimi organi

1. Ponudniki visokotveganih sistemov UI na obrazloženo zahtevo pristojnega nacionalnega organa temu organu zagotovijo vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti visokotvegane sistema UI z zahtevami iz oddelka 2, v enem od uradnih jezikov Unije, ki ga določi zadevna država članica in ga organ brez težav razume.
2. Ponudniki na obrazloženo zahtevo pristojnega organa pristojnemu organu prosilcu po potrebi omogočijo tudi dostop do samodejno ustvarjenih dnevnikov visokotvegane sistema UI iz člena 12(1), če so ti dnevniki pod njihovim nadzorom.
3. Vse informacije, ki jih pristojni organ pridobi na podlagi tega člena, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 22

Pooblaščen zastopniki ponudnikov visokotveganih sistemov UI

1. Ponudniki s sedežem v tretjih državah pred omogočanjem dostopnosti visokotveganih sistemov UI na trgu Unije s pisnim pooblastilom imenujejo pooblaščenega zastopnika s sedežem v Uniji.

2. Ponudnik svojemu pooblaščenemu zastopniku omogoči, da opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika.
3. Pooblaščen zastopnik opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika. Če organi za nadzor trga to zahtevajo, jim predloži izvod pooblastila, in sicer v enem od uradnih jezikov institucij Unije, ki ga navede pristojni organ. Za namene te uredbe pooblastilo pooblaščenemu zastopniku omogoča, da opravlja naslednje naloge:
- (a) preveri, da je bila pripravljena EU izjava o skladnosti iz člena 47 in tehnična dokumentacija iz člena 11 ter da je ponudnik izvedel ustrezen postopek ugotavljanja skladnosti;
 - (b) daje kontaktne podatke ponudnika, ki je določil pooblaščenega zastopnika, izvod EU izjave o skladnosti iz člena 47, tehnično dokumentacijo in, če je ustrezno, certifikat, ki ga je izdal priglašeni organ, na voljo pristojnim organom in nacionalnim organom ali telesom iz člena 74(10) še deset let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo;
 - (c) pristojnemu organu na podlagi obrazložene zahteve zagotovi vse informacije in dokumentacijo, vključno s tisto, ki se hrani v skladu s točko (b) tega pododstavka, potrebne za dokazovanje skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2, vključno z dostopom do dnevnikov, kakor je navedeno v členu 12(1), ki jih samodejno ustvari visokotvegani sistem UI, če so ti dnevniki pod nadzorom ponudnika;

- (d) na podlagi obrazložene zahteve sodeluje s pristojnimi organi pri vseh ukrepih, ki jih ti sprejmejo v zvezi z visokotveganim sistemom UI, zlasti za zmanjšanje in omejitev tveganj, ki jih predstavlja visokotvegani sistem UI;
- (e) po potrebi izpolnjuje obveznosti registracije iz člena 49(1) ali, če registracijo izvede ponudnik sam, zagotovi, da so informacije iz Priloge VIII, oddelek A, točka 3, pravilne.

Na podlagi pooblastila je pooblaščen zastopnik pooblaščen, da lahko pristojni organi nanj, poleg ponudnika ali namesto njega, naslovijo vsa vprašanja, povezana z zagotavljanjem skladnosti s to uredbo.

- 4. Pooblaščen zastopnik odpove pooblastilo, če meni ali utemeljeno domneva, da ponudnik ravna v nasprotju s svojimi obveznostmi iz te uredbe. V takem primeru o odpovedi pooblastila in razlogih zanjo nemudoma obvesti ustrezni organ za nadzor trga in, kadar je primerno, ustrezni priglašeni organ.

Člen 23

Obveznosti uvoznikov

- 1. Pred dajanjem visokotveganega sistema UI na trg uvozniki zagotovijo njegovo skladnost s to uredbo tako, da preverijo, da:
 - (a) je ponudnik za ta visokotvegani sistem UI izvedel ustrezen postopek ugotavljanja skladnosti iz člena 43;

- (b) je ponudnik pripravil tehnično dokumentacijo v skladu s členom 11 in Prilogo IV;
 - (c) je sistem opremljen z zahtevano oznako CE ter so mu priloženi EU izjava o skladnosti iz člena 47 in navodila za uporabo;
 - (d) je ponudnik imenoval pooblaščenega zastopnika v skladu s členom 22(1).
2. Kadar ima uvoznik zadosten razlog za domnevo, da visokotvegani sistem UI ni skladen s to uredbo ali je ponarejen ali mu je priložena ponarejena dokumentacija, tega sistema ne da na trg, dokler ni zagotovljena njegova skladnost. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1), uvoznik o tem obvesti ponudnika sistema, pooblaščenega zastopnika in organe za nadzor trga.
3. Uvozniki na visokotveganem sistemu UI in na embalaži ali v spremni dokumentaciji, kadar je ustrezno, navedejo svoje ime, registrirano trgovsko ime ali registrirano znamko in naslov, na katerem so dosegljivi.
4. Uvozniki zagotovijo, da v času, ko so odgovorni za visokotvegani sistem UI, pogoji skladiščenja ali prevoza, kadar je ustrezno, ne ogrožajo skladnosti sistema z zahtevami iz oddelka 2.

5. Uvozniki še deset let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo, hranijo izvod certifikata, ki ga je izdal priglašeni organ, navodil za uporabo, kadar je to primerno, in EU izjave o skladnosti iz člena 47.
6. Uvozniki ustreznim pristojnim organom na podlagi obrazložene zahteve predložijo vse potrebne informacije in dokumentacijo, vključno s tistimi iz odstavka 5, da dokažejo skladnost visokotvegane sistema UI z zahtevami iz oddelka 2, v jeziku, ki ga organi zlahka razumejo. V ta namen zagotovijo tudi, da se tem organom lahko da na voljo tehnična dokumentacija.
7. Uvozniki sodelujejo z ustreznimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z visokotveganim sistemom UI, ki so ga uvozniki dali na trg, zlasti za zmanjšanje ali omejitev tveganj, ki jih predstavlja ta sistem.

Člen 24

Obveznosti distributerjev

1. Preden omogočijo dostopnost visokotvegane sistema UI na trgu, distributerji preverijo, ali ima zahtevano oznako CE, ali so mu priloženi izvod EU izjave o skladnosti iz člena 47 in navodila za uporabo ter ali sta ponudnik in uvoznik tega sistema, kot je ustrezno, izpolnila vsak svoje obveznosti iz člena 16, točki (b) in (c), oziroma člena 23(3).

2. Kadar distributer meni ali na podlagi informacij, ki jih ima, utemeljeno domneva, da visokotvegani sistem UI ni skladen z zahtevami iz oddelka 2, za visokotvegani sistem UI ne omogoči dostopnosti na trgu, dokler ni zagotovljena skladnost tega sistema z navedenimi zahtevami. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1), distributer o tem obvesti ponudnika oziroma uvoznika sistema, kot je ustrezno.
3. Distributerji zagotovijo, da v času, ko so odgovorni za visokotvegani sistem UI, pogoji skladiščenja ali prevoza, kadar je ustrezno, ne ogrožajo njegove skladnosti z zahtevami iz oddelka 2.
4. Distributer, ki na podlagi informacij, ki jih ima, meni ali utemeljeno domneva, da visokotvegani sistem UI, za katerega je omogočil dostopnost na trgu, ni skladen z zahtevami iz oddelka 2, sprejme popravne ukrepe, potrebne za uskladitev tega sistema z navedenimi zahtevami, ga umakne ali prekliče ali zagotovi, da te popravne ukrepe sprejme ponudnik, uvoznik ali kateri koli zadevni operater, kot je ustrezno. Kadar visokotvegani sistem UI predstavlja tveganje v smislu člena 79(1), distributer o tem nemudoma obvesti ponudnika ali uvoznika sistema in organe, pristojne za zadevni visokotvegani sistem UI, ter navede podrobnosti, zlasti o neskladnosti in vseh sprejetih popravniških ukrepih.

5. Distributerji visokotveganega sistema UI ustreznemu pristojnemu organu na podlagi obrazložene zahteve zagotovijo vse informacije in dokumentacijo o svojih ukrepih na podlagi odstavkov 1 do 4, ki so potrebne za dokazovanje skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2.
6. Distributerji sodelujejo z ustreznimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z visokotveganim sistemom UI, katerega so distributerji dali na trg, zlasti za zmanjšanje ali omejitev tveganja, ki ga predstavlja visokotvegani sistem UI.

Člen 25

Odgovornosti vzdolž verige vrednosti UI

1. Vsak distributer, uvoznik, uvajalec ali druga tretja oseba za namene te uredbe šteje za ponudnika visokotveganega sistema UI in zanj veljajo obveznosti ponudnika iz člena 16 v kateri koli od naslednjih okoliščin:
 - (a) visokotvegani sistem UI, ki je že bil dan na trg ali v uporabo, označijo s svojim imenom ali znamko, brez poseganja v pogodbene dogovore, ki določajo, da so obveznosti drugače dodeljene;
 - (b) bistveno spremenijo visokotvegani sistem UI, ki je že bil dan na trg ali v uporabo, na način, da ostane visokotvegani sistem UI na podlagi člena 6;

- (c) spremenijo predvideni namen sistema UI, vključno s sistemom UI za splošne namene, ki ni bil razvrščen kot sistem visokega tveganja in je že bil dan na trg ali v uporabo na način, da postane visokotvegani sistem UI v skladu s členom 6.
2. Kadar nastopijo okoliščine iz odstavka 1, ponudnik, ki je prvotno dal sistem UI na trg ali v uporabo, za namene te uredbe ne šteje več za ponudnika tega posameznega sistema UI. Ta prvotni ponudnik tesno sodeluje z novimi ponudniki in daje na voljo potrebne informacije ter zagotavlja razumno pričakovani tehnični dostop in drugo pomoč, ki je potrebna za izpolnjevanje obveznosti iz te uredbe, zlasti v zvezi z ugotavljanjem skladnosti visokotveganih sistemov UI. Ta odstavek se ne uporablja v primerih, ko je prvotni ponudnik jasno navedel, da se njegov sistem UI ne sme spremeniti v visokotvegani sistem UI, in zato zanj ne velja obveznost predaje dokumentacije.
3. Za visokotvegane sisteme UI, ki so varnostne komponente proizvodov, za katere se uporablja harmonizacijska zakonodaja Unije iz Priloge I, oddelek A, proizvajalec teh proizvodov šteje za ponudnika visokotvegane sistema UI in zanj veljajo obveznosti iz člena 16 na podlagi enega od naslednjih scenarijev:
- (a) visokotvegani sistem UI se da na trg skupaj s proizvodom pod imenom ali znamko proizvajalca proizvoda;
 - (b) visokotvegani sistem UI se da v uporabo pod imenom ali znamko proizvajalca proizvoda, potem ko je bil ta dan na trg.

4. Ponudnik visokotveganega sistema UI in tretja oseba, ki dobavlja sistem UI, orodja, storitve, komponente ali procese, ki se uporabljajo ali integrirajo v visokotvegani sistem UI, s pisnim dogovorom določita potrebne informacije, zmogljivosti, tehnični dostop in drugo pomoč na podlagi splošno priznanih najsodobnejših tehnoloških dosežkov, da lahko ponudnik visokotveganega sistema UI v celoti izpolnjuje obveznosti iz te uredbe. Ta odstavek se ne uporablja za tretje osebe, ki javnosti omogočajo dostop do orodij, storitev, postopkov ali komponent, ki niso modeli UI za splošne namene, na podlagi proste in odprtokodne licence.

Urad za UI lahko pripravi in priporoči prostovoljne vzorčne pogoje za pogodbe med ponudniki visokotveganih sistemov UI in tretjimi osebami, ki zagotavljajo orodja, storitve, komponente ali postopke, ki se uporabljajo za visokotvegane sisteme UI ali so vanje vključeni. Urad za UI pri oblikovanju teh vzorčnih pogojev upošteva morebitne pogodbene zahteve, ki se uporabljajo v posameznih sektorjih ali poslovnih primerih. Prostovoljni vzorčni pogoji se objavijo in so brezplačno na voljo v lahko uporabni elektronski obliki.

5. Odstavka 2 in 3 ne posegata v potrebo po spoštovanju in varstvu pravic intelektualne lastnine, zaupnih poslovnih informacij in poslovnih skrivnosti v skladu s pravom Unije in nacionalnim pravom.

Člen 26

Obveznosti uvajalcev visokotveganih sistemov UI

1. Uvajalci visokotveganih sistemov UI sprejmejo ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovijo, da uporabljajo take sisteme v skladu s priloženimi navodili za uporabo, na podlagi odstavkov 3 in 6.

2. Uvajalci dodelijo človeški nadzor fizičnim osebam, ki imajo potrebne kompetence, usposobljenost in pooblastila ter potrebno podporo.
3. Obveznosti iz odstavkov 1 in 2 ne posegajo v druge obveznosti uvajalca v skladu s pravom Unije ali nacionalnim pravom ter v pravico uvajalca, da organizira lastna sredstva in dejavnosti za izvajanje ukrepov za človeški nadzor, ki jih navede ponudnik.
4. Brez poseganja v odstavka 1 in 2, če uvajalec izvaja nadzor nad vhodnimi podatki, ta uvajalec zagotovi, da so vhodni podatki ustrezni in dovolj reprezentativni glede na predvideni namen visokotveganega sistema UI.
5. Uvajalci spremljajo delovanje visoko tveganega sistema UI na podlagi navodil za uporabo in po potrebi obvestijo ponudnike v skladu s členom 72. Kadar imajo uvajalci razlog za domnevo, da bi uporaba visoko tveganega sistema UI v skladu z navodili lahko povzročila, da bi visokotvegani sistem UI predstavljal tveganje v smislu člena 79(1), o tem brez nepotrebnega odlašanja obvestijo ponudnika ali distributerja in ustrezni organ za nadzor trga ter začasno prekinejo uporabo tega sistema. Kadar uvajalci odkrijejo resen incident, o tem incidentu takoj obvestijo najprej ponudnika in nato uvoznika ali distributerja in ustrezne organe za nadzor trga. Če uvajalec ne more priti v stik s ponudnikom, se smiselno uporablja člen 73. Ta obveznost ne zajema občutljivih operativnih podatkov uvajalcev sistemov UI, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

Za uvajalce, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, se šteje, da je obveznost spremljanja iz prvega pododstavka izpolnjena z upoštevanjem pravil o ureditvah, procesih in mehanizmi notranjega upravljanja na podlagi ustreznega prava o finančnih storitvah.

6. Uvajalci visokotveganih sistemov UI vodijo dnevnike, ki jih samodejno ustvari ta visokotvegani sistem UI, če so ti dnevniki pod njihovim nadzorom, v obdobju, ki ustreza predvidenemu namenu visokotveganega sistema UI, in sicer vsaj šest mesecev, razen če je v veljavnem pravu Unije ali nacionalnem pravu, zlasti v pravu Unije o varstvu osebnih podatkov, določeno drugače.

Uvajalci, ki so finančne institucije in za katere veljajo zahteve v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki na podlagi prava Unije o finančnih storitvah, vodijo dnevnike kot del dokumentacije, ki se hrani na podlagi ustreznega prava Unije o finančnih storitvah.

7. Uvajalci, ki so delodajalci, pred dajanjem v uporabo ali pred uporabo visokotveganega sistema UI na delovnem mestu obvestijo predstavnike delavcev in delavce, na katere se to nanaša, da se bo zanje uporabljal visokotvegani sistem UI. Te informacije se po potrebi zagotovijo v skladu s pravili in postopki, določenimi v pravu Unije in nacionalnem pravu ter praksi v zvezi z obveščanjem delavcev in njihovih predstavnikov.

8. Uvajalci visokotveganih sistemov UI, ki so javni organi ali institucije, organi, uradi in agencije Unije, izpolnjujejo obveznosti registracije iz člena 49. Če ti uvajalci ugotovijo, da visokotvegani sistem UI, ki ga nameravajo uporabljati, ni bil registriran v podatkovni zbirki EU iz člena 71, tega sistema ne uporabljajo in o tem obvestijo ponudnika ali distributerja.
9. Uvajalci visokotveganih sistemov UI po potrebi uporabijo informacije iz člena 13 te uredbe, da izpolnijo svojo obveznost izvedbe ocene učinka v zvezi z varstvom podatkov na podlagi člena 35 Uredbe (EU) 2016/679 ali člena 27 Direktive (EU) 2016/680.
10. Brez poseganja v Direktivo (EU) 2016/680 v okviru preiskave za ciljno iskanje osebe, ki je osumljena ali obsojena storitve kaznivega dejanja, uvajalec visokotvegane sistema UI za naknadno biometrično identifikacijo na daljavo predhodno ali brez nepotrebnega odlašanja in najpozneje v 48 urah zaprosi sodni organ ali upravni organ, katerega odločitev je zavezujoča in je predmet sodnega nadzora, za uporabo tega sistema, razen če se ta uporablja za prvotno identifikacijo morebitnega osumljenca na podlagi objektivnih in preverljivih dejstev, neposredno povezanih s kaznivim dejanjem. Vsaka uporaba mora biti omejena na tisto, kar je nujno potrebno za preiskavo določenega kaznivega dejanja.

Če se dovoljenje, zahtevano na podlagi prvega pododstavka, zavrne, je treba takoj prenehati uporabljati sistem za naknadno biometrično identifikacijo na daljavo, povezan z zahtevanim dovoljenjem, osebni podatki, povezani z uporabo visokotvegane sistema UI, za katerega je bilo zaproseno dovoljenje, pa se izbrišejo.

V nobenem primeru se tak visokotvegani sistem UI za naknadno biometrično identifikacijo na daljavo ne sme uporabljati za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj na neciljen način, brez kakršne koli povezave s kaznivim dejanjem, kazenskim postopkom, resnično in sedanjostjo ali resnično in predvidljivo grožnjo kaznivega dejanja ali iskanjem določene pogrešane osebe. Zagotovi se, da organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj izključno na podlagi izhodnih podatkov sistema za naknadno biometrično identifikacijo na daljavo ne smejo sprejeti nobene odločitve, ki bi imela negativen pravni učinek na osebo.

Ta odstavek ne posega v člen 9 Uredbe (EU) 2016/679 in člen 10 Direktive (EU) 2016/680 za obdelavo biometričnih podatkov.

Ne glede na namen ali uvajalca se vsaka uporaba takih visokotveganih sistemov UI dokumentira v ustrezni policijski datoteki ter se na zahtevo da na voljo ustreznemu organu za nadzor trga in nacionalnemu organu za varstvo podatkov, razen razkritja občutljivih operativnih podatkov, povezanih s preprečevanjem, odkrivanjem in preiskovanjem kaznivih dejanj. Ta pododstavek ne posega v pooblastila, ki so z Direktivo (EU) 2016/680 dodeljena nadzornim organom.

Uvajalci ustreznim organom za nadzor trga in nacionalnim organom za varstvo podatkov predložijo letna poročila o uporabi sistemov za naknadno biometrično identifikacijo na daljavo, razen razkritja občutljivih operativnih podatkov v zvezi z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Poročila se lahko združijo tako, da zajemajo več kot eno uvedbo.

Države članice lahko v skladu s pravom Unije uvedejo strožje zakone o uporabi sistemov za naknadno biometrično identifikacijo na daljavo.

11. Brez poseganja v člen 50 te uredbe uvajalci visokotveganih sistemov UI iz Priloge III, ki sprejemajo odločitve ali pomagajo pri njihovem odločanju v zvezi s fizičnimi osebami, slednje obvestijo, da se zanje uporablja visokotvegani sistem UI. Za visokotvegane sisteme UI, ki se uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, se uporablja člen 13 Direktive (EU) 2016/680.
12. Uvajalci sodelujejo z ustreznimi pristojnimi organi pri vseh ukrepih, ki jih ti organi sprejmejo v zvezi z visokotveganim sistemom UI, da bi uresničili to uredbo.

Člen 27

Ocena učinka na temeljne pravice za visokotvegane sisteme UI

1. Pred uvedbo visoko tvegane sistema UI iz člena 6(2), razen visokotveganih sistemov UI, namenjenih uporabi na področju iz Priloge III, točka 2, uvajalci, ki so osebe javnega prava ali zasebni subjekti in zagotavljajo javne storitve, ter uvajalci visokotveganih sistemov UI iz Priloge III, točki 5(b) in (c), izvedejo oceno učinka, ki ga lahko povzroči uporaba takega sistema na temeljne pravice. V ta namen uvajalci izvedejo oceno, ki jo sestavljajo:
 - (a) opis postopkov uvajalca, v katerih se bo visokotvegani sistem UI uporabljal v skladu s predvidenim namenom;
 - (b) opis obdobja in pogostosti uporabe vsakega visokotvegane sistema UI;

- (c) kategorije fizičnih oseb in skupin, na katere bo verjetno vplivala njegova uporaba v specifičnem kontekstu;
 - (d) posebna tveganja škode, ki bi lahko vplivala na kategorije fizičnih oseb ali skupine oseb, opredeljene na podlagi tega odstavka, točka (c), ob upoštevanju informacij, ki jih je ponudnik predložil na podlagi člena 13;
 - (e) opis izvajanja ukrepov za človeški nadzor v skladu z navodili za uporabo;
 - (f) ukrepi, ki jih je treba sprejeti, v primeru uresničitve teh tveganj, vključno z ureditvami za notranje upravljanje in pritožbene mehanizme.
2. Obveznost iz odstavka 1 se uporablja za prvo uporabo visokotveganega sistema UI. Uvajalec lahko v podobnih primerih uporabi predhodno izvedeno oceno učinka na temeljne pravice ali obstoječo oceno, ki jo je izvedel ponudnik. Če uvajalec med uporabo visokotveganega sistema UI meni, da se je kateri koli element iz odstavka 1 spremenil ali ni več posodobljen, sprejme potrebne ukrepe za posodobitev informacij.
3. Po izvedbi ocene iz odstavka 1 tega člena uvajalec obvesti organ za nadzor trga o svojih rezultatih, s predložitvijo izpolnjene predloge iz odstavka 5 tega člena. V primeru iz člena 46(1) so lahko uvajalci izvzeti iz obveznosti obveščanja.

4. Če je katera od obveznosti iz tega člena že izpolnjena na podlagi ocene učinka v zvezi z varstvom podatkov, izvedene na podlagi člena 35 Uredbe (EU) 2016/679 ali člena 27 Direktive (EU) 2016/680, ocena učinka na temeljne pravice iz odstavka 1 tega člena dopolnjuje to oceno učinka v zvezi z varstvom podatkov.
5. Urad za UI pripravi predlogo vprašalnika, tudi z avtomatiziranim orodjem, da bi se uvajalcem omogočilo, da na poenostavljen način izpolnijo svoje obveznosti iz tega člena.

ODDELEK 4

PRIGLASITVENI ORGANI IN PRIGLAŠENI ORGANI

Člen 28

Priglasitveni organi

1. Vsaka država članica imenuje ali vzpostavi vsaj en priglasitveni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje. Takšni postopki se oblikujejo v sodelovanju med priglasitvenimi organi vseh držav članic.
2. Države članice lahko odločijo, da mora ocenjevanje in spremljanje iz odstavka 1 izvajati nacionalni akreditacijski organ v smislu Uredbe (ES) št. 765/2008 in v skladu z njo.

3. Priglasitveni organi se ustanovijo, organizirajo in delujejo tako, da ne pride do navzkrižja interesov z organi za ugotavljanje skladnosti ter da se zaščitita objektivnost in nepristranskost njihovih dejavnosti.
4. Priglasitveni organi so organizirani tako, da odločitve v zvezi s priglasitvijo organov za ugotavljanje skladnosti sprejemajo pristojne osebe, ki niso tiste, ki so izvedle ocenjevanje teh organov.
5. Priglasitveni organi ne ponujajo ali izvajajo nobenih dejavnosti, ki jih izvajajo organi za ugotavljanje skladnosti, in tudi nobenih storitev svetovanja na komercialni ali konkurenčni podlagi.
6. Priglasitveni organi zagotavljajo zaupnost pridobljenih informacij v skladu s členom 78.
7. Priglasitveni organi morajo imeti na voljo zadostno število strokovnega osebja za pravilno izvajanje svojih nalog. Pristojno osebje mora imeti potrebno strokovno znanje, kadar je ustrezno, za svojo funkcijo na področjih, kot so informacijske tehnologije, UI in pravo, vključno z nadzorom temeljnih pravic.

Člen 29

Vloga organa za ugotavljanje skladnosti za priglasitev

1. Organi za ugotavljanje skladnosti predložijo vlogo za priglasitev priglasitvenemu organu države članice, v kateri imajo sedež.

2. Vlogi za prigrasitev se priložijo opis dejavnosti ugotavljanja skladnosti, opis modula ali modulov za ugotavljanje skladnosti in opis vrst sistemov UI, za katere organ za ugotavljanje skladnosti trdi, da je zanje pristojen, ter morebitni certifikat o akreditaciji, ki ga izda nacionalni akreditacijski organ, ki potrjuje, da organ za ugotavljanje skladnosti izpolnjuje zahteve iz člena 31.

Dodajo se vsi veljavni dokumenti v zvezi z obstoječimi imenovanji prigrashenega organa vlagatelja na podlagi katere koli druge harmonizacijske zakonodaje Unije.

3. Kadar zadevni organ za ugotavljanje skladnosti ne more zagotoviti certifikata o akreditaciji, prigrasitvenemu organu predloži vsa dokumentarna dokazila, potrebna za preverjanje, priznavanje in redno spremljanje njegove skladnosti z zahtevami iz člena 31.
4. Za prigrasene organe, imenovane na podlagi katere koli druge harmonizacijske zakonodaje Unije, se lahko vsi dokumenti in certifikati v zvezi s temi imenovanji uporabijo za podporo njihovemu postopku imenovanja na podlagi te uredbe, če je to primerno. Prigraseni organ posodobi dokumentacijo iz odstavkov 2 in 3 tega člena, kadar pride do pomembnih sprememb, da bi organu, pristojnemu za prigrasene organe, omogočil spremljanje in preverjanje stalne skladnosti z vsemi zahtevami, določenimi v členu 31.

Člen 30
Postopek priglasitve

1. Priglasitveni organi lahko priglasijo samo tiste organe za ugotavljanje skladnosti, ki izpolnjujejo zahteve iz člena 31.
2. Priglasitveni organi Komisiji in ostalim državam članicam priglasijo vsak organ za ugotavljanje skladnosti iz odstavka 1 z uporabo elektronskega orodja za priglasitev, ki ga je razvila in ga upravlja Komisija.
3. Priglasitev iz odstavka 2 tega člena vključuje vse podrobnosti o dejavnostih ugotavljanja skladnosti, modulu ali modulih za ugotavljanje skladnosti in zadevnih vrstah sistemov UI ter ustrezno potrdilo o usposobljenosti. Kadar priglasitev ne temelji na potrdilu o akreditaciji iz člena 29(2), priglasitveni organ Komisiji in drugim državam članicam predloži dokumentarna dokazila, ki potrjujejo usposobljenost organa za ugotavljanje skladnosti in vzpostavljene ureditve, s čimer se zagotovi, da bo organ redno spremljan in bo še naprej izpolnjeval zahteve iz člena 31.
4. Zadevni organ za ugotavljanje skladnosti lahko izvaja dejavnosti priglašenega organa le, kadar Komisija ali druge države članice ne vložijo ugovora bodisi v dveh tednih od priglasitve s strani priglasitvenega organa, kadar ta vključuje potrdilo o akreditaciji iz člena 29(2), ali v dveh mesecih od priglasitve s strani priglasitvenega organa, kadar ta vključuje dokumentarna dokazila iz člena 29(3).

5. Kadar so vloženi ugovori, se Komisija nemudoma posvetuje z zadevnimi državami članicami in organom za ugotavljanje skladnosti. Glede na to, Komisija odloči, ali je dovoljenje upravičeno ali ne. Svojo odločitev naslovi na zadevno državo članico in ustrezeni organ za ugotavljanje skladnosti.

Člen 31

Zahteve v zvezi s priglašeni organi

1. Priglašeni organ mora biti ustanovljen na podlagi nacionalnega prava države članice in imeti pravno osebnost.
2. Priglašeni organi morajo izpolnjevati organizacijske zahteve, zahteve glede upravljanja kakovosti, virov in procesov, potrebnih za izpolnjevanje njihovih nalog, ter ustrezne zahteve glede kibernetске varnosti.
3. Organizacijska struktura, dodelitev pristojnosti, poročanje in delovanje priglašeni organov morajo zagotavljati zaupanje v učinkovitost priglašeni organov in v rezultate dejavnosti ugotavljanja skladnosti, ki jih izvajajo.
4. Priglašeni organi morajo biti neodvisni od ponudnika visokotveganega sistema UI, v zvezi s katerim izvajajo dejavnosti ugotavljanja skladnosti. Neodvisni morajo biti tudi od vseh drugih operaterjev, ki imajo gospodarski interes pri ocenjevanem visoko tveganem sistemu UI, in od vseh konkurentov ponudnika. To ne izključuje uporabe ocenjenih visokotveganih sistemov UI, nujnih za delovanje organa za ugotavljanje skladnosti, ali uporabe teh sistemov v zasebne namene.

5. Niti organ za ugotavljanje skladnosti in njegovo najvišje vodstvo niti osebje, pristojno za opravljanje nalog ugotavljanja skladnosti, ne smejo neposredno sodelovati pri zasnovi, razvoju, trženju ali uporabi visokotveganih sistemov UI in tudi ne zastopati strani, ki sodelujejo pri teh dejavnostih. Ne smejo sodelovati pri nobeni dejavnosti, ki bi lahko vplivala na njihovo neodvisno presojo ali integriteto v zvezi z dejavnostmi ugotavljanja skladnosti, za katere so priglasi. To zlasti velja za svetovalne storitve.
6. Priglasi organi s svojo organizacijo in delovanjem zagotavljajo neodvisnost, objektivnost in nepristranskost pri izvajanju svojih dejavnosti. Dokumentirajo in izvajajo strukturo in postopke za zagotovitev nepristranskosti ter za spodbujanje in uporabo načel nepristranskosti v svoji organizaciji, med osebjem in v dejavnostih ocenjevanja.
7. Priglasi organi morajo imeti vzpostavljene dokumentirane postopke za zagotovitev, da njihovo osebje, odbori, odvisne družbe, podizvajalci, kateri koli povezan organ ali osebje zunanjih organov v skladu s členom 78 ohranjajo zaupnost informacij, pridobljenih med opravljanjem dejavnosti ugotavljanja skladnosti, razen kadar njihovo razkritje zahteva zakon. Njihovo osebje je zavezano varovanju poklicnih skrivnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog na podlagi te uredbe, razen v zvezi s prigrasitvenimi organi države članice, v kateri izvajajo svoje dejavnosti.

8. Priglašeni organi morajo imeti vzpostavljene postopke za izvajanje dejavnosti, pri katerih se ustrezno upoštevajo velikost ponudnika, sektor, v katerem deluje, njegova struktura in stopnja zahtevnosti zadevnega sistema UI.
9. Priglašeni organi sklenejo ustrezno zavarovanje odgovornosti za svoje dejavnosti ugotavljanja skladnosti, razen če odgovornost prevzame država članica, v kateri imajo sedež, v skladu z nacionalnim pravom ali če je ta država članica sama neposredno pristojna za ugotavljanje skladnosti.
10. Priglašeni organi morajo biti sposobni izvajati vse naloge na podlagi te uredbe z najvišjo stopnjo profesionalne integritete in potrebno usposobljenostjo na določenem področju, ne glede na to, ali navedene naloge izvajajo priglašeni organi sami ali se izvajajo v njihovem imenu in pod njihovo odgovornostjo.
11. Priglašeni organi morajo imeti zadostne notranje kompetence, da lahko učinkovito ocenijo naloge, ki jih opravljajo zunanje stranke v njihovem imenu. Stalno morajo imeti na voljo dovolj upravnega, tehničnega, pravnega in znanstvenega osebja, ki ima izkušnje in znanje v zvezi z ustreznimi vrstami sistemov UI, podatki in računalniško obdelavo podatkov ter v zvezi z zahtevami iz oddelka 2.
12. Priglašeni organi sodelujejo v usklajevalnih dejavnostih iz člena 38. Sodelujejo tudi neposredno v evropskih organizacijah za standardizacijo ali so v njih zastopani oziroma zagotavljajo, da so seznanjeni z ustreznimi standardi in na tekočem z njimi.

Člen 32

Domneva o skladnosti z zahtevami v zvezi s priglašeni organi

Kadar organ za ugotavljanje skladnosti dokaže svojo skladnost z merili, določenimi v ustreznih harmoniziranih standardih ali njihovih delih, katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*, se domneva, da izpolnjuje zahteve iz člena 31, kolikor so te zajete v veljavnih harmoniziranih standardih.

Člen 33

Odvisne družbe priglašeni organov in podizvajanje

1. Kadar priglašeni organ določene naloge, povezane z ugotavljanjem skladnosti, odda v izvajanje podizvajalcu ali jih prenese na odvisno družbo, zagotovi, da podizvajalec oziroma odvisna družba izpolnjuje zahteve iz člena 31, ter o tem obvesti priglasitveni organ.
2. Priglašeni organi so v celoti odgovorni za naloge, ki jih izvajajo kateri koli podizvajalci ali odvisne družbe.
3. Dejavnosti se lahko prenesejo na podizvajalca ali odvisno družbo samo, če ponudnik s tem soglaša. Priglašeni organi objavijo seznam svojih podizvajalcev.
4. Zadevni dokumenti v zvezi z ocenjevanjem usposobljenosti podizvajalca ali odvisne družbe in delom, ki ga izvaja na podlagi te uredbe, so na voljo priglasitvenemu organu pet let od datuma zaključka podizvajanja.

Člen 34

Operativne obveznosti priglašениh organov

1. Priglašeni organi preverijo skladnost visokotveganih sistemov UI v skladu s postopki ugotavljanja skladnosti iz člena 43.
2. Priglašeni organi se pri opravljanju svojih dejavnosti izogibajo ustvarjanju nepotrebnih bremen za ponudnike ter ustrezno upoštevajo velikost ponudnika, sektor, v katerem deluje, njegovo strukturo in stopnjo kompleksnosti zadevnega visokotveganega sistema UI, zlasti zato, da bi čim bolj zmanjšali upravna bremena in stroške izpolnjevanja obveznosti za mikro in mala podjetja v smislu Priporočila 2003/361/ES. Vendar upoštevajo stopnjo rigoroznosti in raven zaščite, ki sta potrebni za skladnost visokotveganega sistema UI z zahtevami te uredbe.
3. Priglašeni organi dajo priglasitvenemu organu iz člena 28 na voljo vso zadevno dokumentacijo – vključno z dokumentacijo ponudnikov –, ki mu jo na zahtevo tudi predložijo, da temu organu omogočijo izvajanje dejavnosti ocenjevanja, imenovanja, priglasitve in spremljanja ter da se olajša ocenjevanje, opisano v tem oddelku.

Člen 35

Identifikacijske številke in sezname priglašениh organov

1. Komisija vsakemu priglašenemu organu dodeli enotno identifikacijsko številko, tudi kadar je organ priglašen na podlagi več kot enega akta Unije.

2. Komisija objavi seznam organov, priglašanih na podlagi te uredbe, vključno z njihovimi identifikacijskimi številkami in dejavnostmi, za katere so bili priglašeni. Komisija skrbi za posodabljanje seznama.

Člen 36

Spremembe prigrasitev

1. Prigrasitveni organ uradno obvesti Komisijo in druge države članice o vseh pomembnih spremembah prigrasitve priglašene organa z uporabo elektronskega orodja za prigrasitev iz člena 30(2).
2. Postopki iz členov 29 in 30 se uporabljajo za razširitev področja uporabe prigrasitve.

Za druge spremembe prigrasitve, razen za razširitev njenega področja uporabe, se uporabljajo postopki iz odstavkov 3 do 9.
3. Kadar priglašeni organ sklene, da bo prenehal izvajati dejavnosti za ugotavljanje skladnosti, o tem obvesti prigrasitveni organ in zadevne ponudnike čim prej, v primeru načrtovanega prenehanja pa vsaj eno leto pred prenehanjem izvajanja svojih dejavnosti. Certifikati priglašene organa lahko ostanejo veljavni devet mesecev po prenehanju njegovih dejavnosti, pod pogojem da je drug priglašeni organ pisno potrdil, da bo prevzel odgovornost za visokotvegane sisteme UI, na katere se ti certifikati nanašajo. Slednji priglašeni organ opravi celovito oceno zadevnih visokotveganih sistemov UI do konca tega devetmesečnega obdobja, preden izda nove certifikate za te sisteme. Kadar priglašeni organ preneha opravljati svojo dejavnost, prigrasitveni organ imenovanje umakne.

4. Kadar ima prigrasitveni organ zadosten razlog za domnevo, da prigraseni organ ne izpolnjuje več zahtev iz člena 31 ali da ne izpolnjuje svojih obveznosti, zadevo brez odlašanja razišče z največjo skrbnostjo. V tem okviru obvesti zadevni prigraseni organ o vloženih ugovorih in mu omogoči, da izrazi svoja stališča. Če prigrasitveni organ ugotovi, da prigraseni organ ne izpolnjuje več zahtev iz člena 31 ali ne izpolnjuje svojih obveznosti, omeji, začasno prekliče ali umakne imenovanje, odvisno od resnosti neizpolnjevanja navedenih zahtev ali neizpolnjevanja navedenih obveznosti. O tem nemudoma obvesti Komisijo in druge države članice.
5. Kadar se imenovanje prigrasenega organa začasno prekliče, omeji oziroma v celoti ali delno umakne, prigraseni organ o tem obvesti zadevne ponudnike v desetih dneh.
6. V primeru omejitve, začasnega preklica ali umika imenovanja prigrasitveni organ izvede ustrezne ukrepe za zagotovitev, da se dokumentacija zadevnega prigrasenega organa ohrani in je na voljo prigrasitvenim organom v drugih državah članicah ter organom, pristojnim za nadzor trga, če to zahtevajo.
7. V primeru omejitve, začasnega preklica ali umika imenovanja prigrasitveni organ:
 - (a) oceni vpliv na certifikate, ki jih je izdal prigraseni organ;
 - (b) Komisiji in drugim državam članicam v treh mesecih od uradnega obvestila o spremembah imenovanja predloži poročilo o svojih ugotovitvah;

- (c) od priglasičenega organa zahteva, da v razumnem časovnem roku, ki ga določi organ, začasno prekliče ali umakne vse neupravičeno izdane certifikate, da se zagotovi kontinuirana skladnost visokotveganih sistemov UI na trgu;
- (d) Komisijo in države članice obvesti o certifikatih, katerih začasni preklic ali umik je zahteval;
- (e) pristojnim nacionalnim organom države članice, v kateri ima ponudnik registriran sedež poslovanja, zagotovi vse ustrezne informacije o certifikatih, katerih začasni preklic ali umik je zahteval; ta organ sprejme ustrezne ukrepe za preprečitev morebitnega tveganja za zdravje, varnost ali temeljne pravice, kadar je to potrebno.

8. Razen neupravičeno izdanih certifikatov ostanejo certifikati, kadar je bilo imenovanje začasno preklicano ali omejeno, veljavni v naslednjih okoliščinah:

- (a) priglasičveni organ je v enem mesecu od začasnega preklica ali omejitve potrdil, da v zvezi s certifikati, za katere velja začasni preklic ali omejitev, ni nobenega tveganja za zdravje, varnost ali temeljne pravice, ter določil časovni potek za ukrepe, potrebne za odpravo začasnega preklica ali omejitve, ali

- (b) priglasitveni organ je potrdil, da v obdobju začasnega preklica ali omejitve ne bo izdan, spremenjen ali ponovno izdan noben certifikat, povezan z začasnim preklicem, hkrati pa navedel, ali je priglašeni organ v obdobju začasnega preklica ali omejitve še vedno sposoben spremljati veljavne izdane certifikate in zanje odgovarjati; če priglasitveni organ ugotovi, da priglašeni organ ni sposoben zagotavljati podpore za veljavne izdane certifikate, ponudnik sistema, na katerega se nanaša certifikat, pristojnim nacionalnim organom države članice, v kateri ima registrirani sedež poslovanja, v treh mesecih od začasnega preklica ali omejitve pisno potrdi, da drug kvalificiran priglašeni organ začasno prevzema naloge priglašene organa v smislu spremljanja certifikatov in odgovarjanja zanje v obdobju začasnega preklica ali omejitve.

9. Razen v primeru neupravičeno izdanih certifikatov in kadar je bilo imenovanje umaknjeno, ostanejo certifikati v naslednjih okoliščinah veljavni še devet mesecev:

- (a) pristojni nacionalni organ države članice, v kateri ima ponudnik visoko tveganega sistema UI, na katerega se nanaša certifikat, registrirani sedež poslovanja, je potrdil, da v povezavi z zadevnimi visokotveganimi sistemi UI ni tveganja za zdravje, varnost ali temeljne pravice, ter
- (b) drug priglašeni organ je pisno potrdil, da bo takoj prevzel odgovornost za te sisteme UI in v 12 mesecih od umika imenovanja zaključi njihovo ocenjevanje.

V okoliščinah iz prvega pododstavka sme pristojni nacionalni organ države članice, v kateri ima ponudnik sistema, na katerega se nanaša certifikat, sedež poslovanja, podaljšati začasno veljavnost certifikatov za nadaljnja obdobja treh mesecev, ki pa skupaj ne smejo trajati dlje kot dvanajst mesecev.

Pristojni nacionalni organ ali priglašeni organ, ki prevzame naloge priglašene organa, na katerega se nanaša sprememba imenovanja, o tem takoj obvesti Komisijo, druge države članice in druge priglašene organe.

Člen 37

Izpodbijanje usposobljenosti priglašениh organov

1. Komisija po potrebi razišče vse primere, v katerih obstajajo razlogi za dvom v usposobljenost priglašene organa oziroma ali priglašeni organ še vedno izpolnjuje zahteve iz člena 31 in svoje veljavne obveznosti.
2. Priglasitveni organ Komisiji na zahtevo predloži vse ustrezne informacije v zvezi s priglasitvijo ali vzdrževanjem usposobljenosti zadevnega priglašene organa.
3. Komisija zagotovi, da se vse občutljive informacije, ki jih pridobi med preiskavami na podlagi tega člena, obravnavajo zaupno v skladu s členom 78.

4. Kadar Komisija ugotovi, da priglašeni organ ne izpolnjuje ali ne izpolnjuje več zahtev za prigrasitev, o tem ustrezno obvesti državo članico prigrasiteljico in od nje zahteva, da sprejme potrebne popravne ukrepe, po potrebi vključno z začasnim preklicem ali umikom prigrasitve. Kadar država članica ne sprejme potrebnih popravnih ukrepov, lahko Komisija z izvedbenim aktom začasno prekliče, omeji ali umakne imenovanje. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).

Člen 38

Usklajevanje prigrasjenih organov

1. Komisija zagotovi, da se v zvezi z visokotveganimi sistemi UI vzpostavi ustrezno usklajevanje in sodelovanje med prigrasjenimi organi, dejavnimi v postopkih ugotavljanja skladnosti na podlagi te uredbe, ter da se to usklajevanje in sodelovanje pravilno izvajata v obliki sektorske skupine prigrasjenih organov.
2. Vsak prigrasitveni organ zagotovi, da organi, ki jih prigrasi, neposredno ali prek imenovanih predstavnikov sodelujejo pri delu skupine iz odstavka 1.
3. Komisija omogoči izmenjavo znanja in primerov najboljših praks med prigrasitvenimi organi.

Člen 39

Organi za ugotavljanje skladnosti iz tretjih držav

Organi za ugotavljanje skladnosti, ustanovljeni na podlagi prava tretje države, s katero je Unija sklenila sporazum, so lahko pooblaščen za izvajanje dejavnosti priglašeni organov na podlagi te uredbe, če izpolnjujejo zahteve iz člena 31 ali zagotavljajo enakovredno raven izpolnjevanja zahtev.

ODDELEK 5

STANDARDI, UGOTAVLJANJE SKLADNOSTI, CERTIFIKATI, REGISTRACIJA

Člen 40

Harmonizirani standardi in standardizacijski dokumenti

1. Za visokotvegane sisteme UI ali modele UI za splošne namene, ki so skladni s harmoniziranimi standardi ali njihovimi deli, katerih sklici so bili objavljeni v *Uradnem listu Evropske unije* v skladu z Uredbo (EU) št. 1025/2012, se domneva, da so skladni z zahtevami iz oddelka 2 tega poglavja ali, kot je ustrezno, z obveznostmi iz poglavja V, oddelka 2 in 3, te uredbe, kolikor ti standardi zajemajo te zahteve ali obveznosti.

2. Komisija v skladu s členom 10 Uredbe (EU) št. 1025/2012 brez nepotrebnega odlašanja izda zahteve za standardizacijo, ki zajemajo vse zahteve iz oddelka 2 tega poglavja in, kot je ustrezno, zahteve za standardizacijo, ki zajemajo obveznosti iz poglavja V, oddelka 2 in 3, te uredbe. V zahtevi za standardizacijo se zahtevajo tudi dokumenti v zvezi s postopki poročanja in dokumentiranja za izboljšanje učinkovitosti virov sistemov UI, kot je zmanjšanje porabe energije in drugih virov visokotveganega sistema UI v njegovem življenjskem ciklu, ter dokumenti v zvezi z energijsko učinkovitim razvojem modelov UI za splošne namene. Komisija se pri pripravi zahteve za standardizacijo posvetuje z Odborom in ustreznimi deležniki, vključno s svetovalnim forumom.

Komisija pri izdaji zahteve za standardizacijo evropskim organizacijam za standardizacijo določi, da morajo biti standardi jasni, skladni, tudi s standardi, razvitimi v različnih sektorjih, za proizvode, za katere velja obstoječa harmonizacijska zakonodaja Unije iz Priloge I, in namenjeni temu, da se zagotovi, da visokotvegani sistemi UI ali modeli UI za splošne namene, ki so dani na trg ali v uporabo v Uniji, izpolnjujejo ustrezne zahteve ali obveznosti iz te uredbe.

Komisija od evropskih organizacij za standardizacijo zahteva, da v skladu s členom 24 Uredbe (EU) št. 1025/2012 predložijo dokaze o svojih najboljših prizadevanjih za izpolnitev ciljev iz prvega in drugega pododstavka tega odstavka.

3. Udeleženci v postopku standardizacije si prizadevajo spodbujati naložbe in inovacije na področju UI, tudi s krepitevijo pravne varnosti, ter konkurenčnost in rast trga Unije, prispevati k izboljšanju globalnega sodelovanja na področju standardizacije ob upoštevanju obstoječih mednarodnih standardov na področju UI, ki so skladni z vrednotami, temeljnimi pravicami in interesi Unije, ter krepi večdeležniško upravljanje, pri čemer zagotavljajo uravnoteženo zastopnost interesov in učinkovito sodelovanje vseh ustreznih deležnikov v skladu s členi 5, 6 in 7 Uredbe (EU) št. 1025/2012.

Člen 41

Skupne specifikacije

1. Komisija lahko sprejme izvedbene akte o določitvi skupnih specifikacij za zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, za obveznosti iz oddelkov 2 in 3 poglavja V, kadar so izpolnjeni naslednji pogoji:
- (a) Komisija je na podlagi člena 10(1) Uredbe (EU) št. 1025/2012 zahtevala, da ena ali več evropskih organizacij za standardizacijo pripravi osnutek harmoniziranega standarda za zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, za obveznosti iz oddelkov 2 in 3 poglavja V, in:
- (i) zahteve ni sprejela nobena evropska organizacija za standardizacijo ali

- (ii) harmonizirani standardi, ki se nanašajo na to zahtevo, niso bili predloženi v roku, določenem v skladu s členom 10(1) Uredbe (EU) št. 1025/2012, ali
 - (iii) v ustreznih harmoniziranih standardih so nezadostno obravnavani pomisleki glede temeljnih pravic ali
 - (iv) harmonizirani standardi niso skladni z zahtevo ter
- (b) v *Uradnem listu Evropske unije* v skladu z Uredbo (EU) št. 1025/2012 ni objavljen sklic na harmonizirane standarde, ki zajemajo zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, obveznosti iz oddelkov 2 in 3 poglavja V, in objava takega sklica se v razumnem roku tudi ne pričakuje.

Pri pripravi skupnih specifikacij se Komisija posvetuje s svetovalnim forumom iz člena 67.

Izvedbeni akti iz prvega pododstavka tega odstavka se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

2. Komisija pred pripravo osnutka izvedbenega akta obvesti odbor iz člena 22 Uredbe (EU) št. 1025/2012, da meni, da so pogoji iz odstavka 1 tega člena izpolnjeni.

3. Za visokotvegane sisteme UI ali modele UI za splošne namene, ki so v skladu s skupnimi specifikacijami iz odstavka 1 ali deli navedenih specifikacij, se domneva, da so skladni z zahtevami iz oddelka 2 tega poglavja ali, kot je ustrezno, izpolnjujejo zahteve iz oddelkov 2 in 3 poglavja V, kolikor so te zajete v teh skupnih specifikacijah ali teh obveznostih.
4. Kadar evropska organizacija za standardizacijo sprejme harmonizirani standard in ga predloži Komisiji, da se sklic nanj objavi v *Uradnem listu Evropske unije*, Komisija harmonizirani standard oceni v skladu z Uredbo (EU) št. 1025/2012. Ko se sklic na harmonizirani standard objavi v *Uradnem listu Evropske unije*, Komisija razveljavi izvedbene akte iz odstavka 1 ali njihove dele, ki zajemajo zahteve, enake zahtevam iz oddelka 2 tega poglavja ali, kot je ustrezno, iste obveznosti iz oddelkov 2 in 3 poglavja V.
5. Kadar ponudniki visokotveganih sistemov UI ali modelov UI za splošne namene ne izpolnjujejo skupnih specifikacij iz odstavka 1, ustrezno utemeljijo, da so sprejeli tehnične rešitve, ki izpolnjujejo zahteve iz oddelka 2 tega poglavja ali, kot je ustrezno, izpolnjujejo obveznosti iz oddelkov 2 in 3 poglavja V v tolikšni meri, da so jim vsaj enakovredne.

6. Kadar država članica meni, da skupna specifikacija ne izpolnjuje v celoti zahtev iz oddelka 2 ali, kot je ustrezno, ne izpolnjuje obveznosti iz oddelkov 2 in 3 poglavja V, o tem s podrobno obrazložitvijo obvesti Komisijo. Komisija te informacije oceni in po potrebi spremeni izvedbeni akt o določitvi zadevne skupne specifikacije.

Člen 42

Domneva o skladnosti z nekaterimi zahtevami

1. Za visokotvegane sisteme UI, ki so bili naučeni in testirani na podlagi podatkov, ki odražajo posebno geografsko, vedenjsko, kontekstualno ali funkcionalno okolje, v katerem naj bi se uporabljali, se domneva, da izpolnjujejo ustrezne zahteve iz člena 10(4).
2. Za visokotvegane sisteme UI, ki so prejeli potrdilo ali za katere je bila izdana izjava o skladnosti v okviru sheme za kibernetško varnost na podlagi Uredbe (EU) 2019/881, sklici na katero so bili objavljeni v *Uradnem listu Evropske unije*, se domneva, da izpolnjujejo zahteve za kibernetško varnost iz člena 15 te uredbe, kolikor so te zahteve zajete v certifikatu o kibernetški varnosti ali izjavi o skladnosti ali v njunih delih.

Člen 43
Ugotavljanje skladnosti

1. Za visokotvegane sisteme UI iz Priloge III, točka 1, pri katerih je ponudnik pri dokazovanju skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2 uporabil harmonizirane standarde iz člena 40 ali, kadar je to primerno, skupne specifikacije iz člena 41, ponudnik izbere enega od naslednjih postopkov za ugotavljanje skladnosti na podlagi:
- (a) notranjega nadzora iz Priloge VI ali
 - (b) ocenjevanja sistema upravljanja kakovosti in ocenjevanja tehnične dokumentacije s sodelovanjem priglasičenega organa iz Priloge VII.

Pri dokazovanju skladnosti visokotveganega sistema UI z zahtevami iz oddelka 2 ponudnik opravi postopek ugotavljanja skladnosti iz Priloge VII, kadar:

- (a) harmonizirani standardi iz člena 40 ne obstajajo in skupne specifikacije iz člena 41 niso na voljo;
- (b) ponudnik ni uporabil harmoniziranega standarda ali ga je uporabil le delno;
- (c) skupne specifikacije iz točke (a) obstajajo, vendar jih ponudnik ni uporabil;

- (d) je bil eden ali več harmoniziranih standardov iz točke (a) objavljen z omejitvijo in samo za tisti del standarda, ki je bil omejen.

Za namene postopka ugotavljanja skladnosti iz Priloge VII lahko ponudnik izbere katerega koli od priglašeni organov. Kadar pa naj bi visokotvegani sistem UI dali v uporabo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali azilni organi ali institucije, organi, uradi in agencije Unije, je priglašen organ organ za nadzor trga iz člena 74(8) ali (9), kot je ustrezno.

2. Za visokotvegane sisteme UI iz Priloge III, točke 2 do 8, ponudniki upoštevajo postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI, ki ne predvideva sodelovanja priglašene organa.
3. Za visokotvegane sisteme UI, zajete v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, ponudnik upošteva ustrezni postopek ugotavljanja skladnosti, kot se zahteva v navedenih pravnih aktih. Za te visokotvegane sisteme UI se uporabljajo zahteve iz oddelka 2 tega poglavja, ki so del te ocene. Uporablja se tudi Priloga VII, točke 4.3, 4.4, 4.5 in peti odstavek točke 4.6.

Za namene te ocene so priglašeni organi, ki so priglašeni na podlagi teh pravnih aktov, upravičeni nadzorovati skladnost visokotveganih sistemov UI z zahtevami iz oddelka 2, če je bila skladnost teh priglašeni organov z zahtevami iz člena 31(4), (5), (10) in (11) ocenjena v okviru postopka priglasitve na podlagi teh pravnih aktov.

Kadar pravni akt iz Priloge I, oddelek A, proizvajalcu proizvoda omogoča, da se odloči za izvzetje iz ugotavljanja skladnosti s strani tretjih oseb, pod pogojem, da je ta proizvajalec uporabil vse harmonizirane standarde, ki zajemajo vse ustrezne zahteve, lahko ta proizvajalec uporabi to možnost le, če je uporabil harmonizirane standarde ali, kadar je to primerno, skupne specifikacije iz člena 41, ki zajemajo vse zahteve iz oddelka 2 tega poglavja.

4. Pri visokotveganih sistemih UI, pri katerih je bil že opravljen postopek ugotavljanja skladnosti, se v primeru bistvene spremembe opravi nov postopek ugotavljanja skladnosti, ne glede na to, ali je spremenjeni sistem namenjen nadaljnji distribuciji ali ga še naprej uporablja sedanji uvajalec.

Za visokotvegane sisteme UI, ki se po dajanju na trg ali v uporabo še naprej učijo, spremembe visokotvegane sistema UI in njegove zmogljivosti, ki jih je ponudnik vnaprej določil ob začetnem ugotavljanju skladnosti in so del informacij iz tehnične dokumentacije iz Priloge IV, točka 2(f), ne pomenijo bistvene spremembe.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da zaradi tehničnega napredka spremeni s posodobitvijo prilogi VI in VII.

6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97 za spremembo odstavkov 1 in 2 tega člena, da se za visokotvegane sisteme UI iz Priloge III, točke 2 do 8, v celoti ali deloma uvede postopek ugotavljanja skladnosti iz Priloge VII. Komisija take delegirane akte sprejme ob upoštevanju učinkovitosti postopka ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI pri preprečevanju ali čim večjem zmanjševanju tveganj za zdravje in varnost ter varstvo temeljnih pravic, ki jih predstavljajo taki sistemi, ter razpoložljivosti ustreznih zmogljivosti in virov med priglašeni organi.

Člen 44

Certifikati

1. Certifikati, ki jih izdajo priglašeni organi v skladu s Prilogo VII, so sestavljeni v jeziku, ki ga ustrezni organi v državi članici, v kateri ima priglašeni organ sedež, zlahka razumejo.
2. Certifikati so veljavni toliko časa, kolikor je navedeno, a ne več kot pet let za sisteme UI iz Priloge I in štiri leta za sisteme UI iz Priloge III. Na zahtevo ponudnika se lahko veljavnost certifikata na podlagi ponovne ocene v skladu z veljavnimi postopki za ugotavljanje skladnosti podaljša za nadaljnja obdobja, ki ne presegajo pet let za sisteme UI iz Priloge II in štirih let za sisteme UI iz Priloge III. Vsako dopolnilo k certifikatu ostane veljavno, če je veljaven certifikat, ki ga to dopolnjuje.

3. Kadar priglašeni organ ugotovi, da sistem UI ne izpolnjuje več zahtev iz oddelka 2, ob upoštevanju načela sorazmernosti začasno prekliče ali umakne izdan certifikat oziroma ga omeji, razen če se skladnost s temi zahtevami zagotovi z ustreznimi popravnimi ukrepi, ki jih je ponudnik sistema sprejel v ustreznem roku, ki ga je določil priglašeni organ. Priglašeni organ svojo odločitev obrazloži.

Zoper odločitve priglašениh organov, tudi o izdanih certifikatih o skladnosti, je na voljo pritožbeni postopek.

Člen 45

Obveznosti obveščanja za priglašene organe

1. Priglašeni organi obvestijo priglasitveni organ:
 - (a) o vsakem certifikatu Unije o oceni tehnične dokumentacije, vsakem dodatku k tem certifikatom in vsaki odobritvi sistema upravljanja kakovosti, ki se izdajo v skladu z zahtevami iz Priloge VII;
 - (b) o vsaki zavrnitvi, omejitvi, začasnem preklicu ali umiku certifikata Unije o oceni tehnične dokumentacije ali odobritve sistema upravljanja kakovosti, ki se izda v skladu z zahtevami iz Priloge VII;
 - (c) o vsaki okoliščini, ki vpliva na obseg ali pogoje za prigrasitev;

- (d) o vsaki zahtevi za informacije, ki so jo prejeli od organov za nadzor trga, v zvezi z dejavnostmi ugotavljanja skladnosti;
- (e) na zahtevo o dejavnostih ugotavljanja skladnosti, izvedenih v okviru njihove priglasitve, in vsaki drugi izvedeni dejavnosti, vključno s čezmejnimi dejavnostmi in sklepanjem pogodb s podizvajalci.

2. Vsak priglašeni organ obvesti druge priglašene organe:

- (a) o odobritvah sistema upravljanja kakovosti, ki jih je zavrnil, začasno preklical ali umaknil, ter na zahtevo o odobritvah sistema upravljanja kakovosti, ki jih je izdal;
- (b) o certifikatih Unije o oceni tehnične dokumentacije ali njihovih dodatkih, ki jih je zavrnil, začasno preklical, umaknil ali drugače omejil, ter na zahtevo o certifikatih in/ali njihovih dodatkih, ki jih je izdal.

3. Vsak priglašeni organ drugim priglašenim organom, ki izvajajo podobne dejavnosti ugotavljanja skladnosti za iste vrste sistemov UI, predloži ustrezne informacije o vprašanjih v zvezi z negativnimi rezultati ugotavljanja skladnosti, na zahtevo pa tudi v zvezi s pozitivnimi.

4. Priglasitveni organi zagotavljajo zaupnost pridobljenih informacij v skladu s členom 78.

Člen 46

Odstopanje od postopka ugotavljanja skladnosti

1. Z odstopanjem od člena 43 in na podlagi ustrezno utemeljene zahteve lahko kateri koli organ za nadzor trga dovoli dajanje posebnih visokotveganih sistemov UI na trg ali v uporabo na ozemlju zadevne države članice iz izjemnih razlogov javne varnosti ali varstva življenja in zdravja ljudi, varstva okolja ter varstva ključnih industrijskih in infrastrukturnih sredstev. To dovoljenje velja omejeno obdobje, dokler se izvajajo potrebni postopki ugotavljanja skladnosti, ob upoštevanju izjemnih razlogov, ki upravičujejo odstopanje. Ti postopki se zaključijo brez nepotrebnega odlašanja.
2. V ustrezno utemeljenih nujnih primerih iz izjemnih razlogov javne varnosti ali v primeru posebne, precejšnje in neposredne grožnje za življenje ali telesno varnost fizičnih oseb lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali organi civilne zaščite dajo določen visokotvegani sistem UI v uporabo brez dovoljenja iz odstavka 1, če se za tako dovoljenje brez nepotrebnega odlašanja zaprosi med uporabo ali po njej. Če se dovoljenje iz odstavka 1 zavrne, se uporaba visokotvegane sistema UI takoj ustavi, vsi rezultati in izhodni podatki, ki izhajajo iz take uporabe, pa se takoj zavržejo.

3. Dovoljenje iz odstavka 1 se izda le, če organ za nadzor trga ugotovi, da visokotvegani sistem UI izpolnjuje zahteve iz oddelka 2. Organ za nadzor trga obvesti Komisijo in druge države članice o vseh dovoljenjih, izdanih na podlagi odstavkov 1 in 2. Ta obveznost ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.
4. Kadar v 15 koledarskih dneh po prejemu informacij iz odstavka 3 država članica ali Komisija ne poda nobenega ugovora glede dovoljenja, ki ga je izdal organ za nadzor trga države članice v skladu z odstavkom 1, se šteje, da je dovoljenje upravičeno.
5. Kadar v 15 koledarskih dneh po prejemu obvestila iz odstavka 3 država članica poda ugovore zoper dovoljenje, ki ga je izdal organ za nadzor trga druge države članice, ali kadar Komisija meni, da je dovoljenje v nasprotju s pravom Unije ali da je sklep držav članic glede skladnosti sistema iz odstavka 3 neutemeljen, se Komisija brez odlašanja posvetuje z zadevno državo članico. Z zadevnimi operaterji se posvetuje in ti imajo možnost, da predstavijo svoja stališča. Glede na to Komisija odloči, ali je dovoljenje upravičeno. Komisija svojo odločitev sporoči zadevnim državam članicam in ustreznim operaterjem.
6. Kadar Komisija meni, da je dovoljenje neupravičeno, ga organ za nadzor trga zadevne države članice umakne.

7. Za visokotvegane sisteme UI, povezane s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, se uporabljajo samo odstopanja od ugotavljanja skladnosti, določena v navedeni harmonizacijski zakonodaji Unije.

Člen 47

EU izjava o skladnosti

1. Ponudnik za vsak visokotvegani sistem UI sestavi strojno berljivo, fizično ali elektronsko podpisano pisno EU izjavo o skladnosti in jo hrani za potrebe pristojnih nacionalnih organov ter jim jo daje na voljo še 10 let po tem, ko je bil visokotvegani sistem UI dan na trg ali v uporabo. V EU izjavi o skladnosti se opredeli, za kateri visokotvegani sistem UI je bila sestavljena. Na zahtevo se ustreznim pristojnim nacionalnim organom predloži izvod EU izjave o skladnosti.
2. V EU izjavi o skladnosti se navede, da zadevni visokotvegani sistem UI izpolnjuje zahteve iz oddelka 2. EU izjava o skladnosti vsebuje informacije iz Priloge V in se prevede v jezik, ki ga pristojni nacionalni organi držav članic, v katerih je visokotvegani sistem UI dan na trg ali je omogočena dostopnost do njega, zlahka razumejo.

3. Kadar za visokotvegane sisteme UI velja druga harmonizacijska zakonodaja Unije, v skladu s katero se zahteva tudi EU izjava o skladnosti, se pripravi enotna EU izjava o skladnosti za pravo Unije, ki se uporablja za visokotvegani sistem UI. Ta izjava vsebuje vse informacije, s katerimi se ugotovi, na katero harmonizacijsko zakonodajo Unije se izjava nanaša.
4. S pripravo EU izjave o skladnosti ponudnik prevzame odgovornost za skladnost z zahtevami iz oddelka 2. Ponudnik EU izjavo o skladnosti, če je to primerno, posodablja.
5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da se spremeni Priloga V, s posodobitvijo vsebine EU izjave o skladnosti iz navedene priloge, da se uvedejo elementi, potrebni zaradi tehničnega napredka.

Člen 48

Oznaka CE

1. Za oznako CE veljajo splošna načela iz člena 30 Uredbe (ES) št. 765/2008.
2. Za visokotvegane sisteme UI, ki se zagotavljajo digitalno, se digitalna oznaka CE uporablja le, če je do nje mogoče enostavno dostopati prek vmesnika, prek katerega se dostopa do tega sistema, ali prek lahko dostopne strojno berljive kode ali drugega elektronskega sredstva.

3. Oznaka CE se vidno, čitljivo in neizbrisno namesti na visokotvegane sisteme UI. Kadar to ni mogoče ali ni upravičeno zaradi značilnosti visokotveganega sistema UI, se oznaka namesti bodisi na embalažo ali na priloženo dokumentacijo.
4. Kadar je to primerno, oznaki CE sledi identifikacijska številka priglašenega organa, odgovornega za postopke ugotavljanja skladnosti iz člena 43. Identifikacijsko številko priglašenega organa pritrdi organ sam ali pa jo na podlagi njegovih navodil pritrdi ponudnik ali njegov pooblaščen zastopnik. Identifikacijska številka se navede tudi v promocijskem gradivu, v katerem je omenjeno, da visokotvegani sistem UI izpolnjuje zahteve za oznako CE.
5. Kadar visokotvegane sisteme UI ureja drugo pravo Unije, ki prav tako določa namestitvev oznake CE, se na tej oznaki navede, da visokotvegani sistem UI izpolnjuje tudi zahteve tega drugega prava.

Člen 49

Registracija

1. Pred dajanjem visokotveganega sistema UI iz Priloge III, z izjemo visokotveganih sistemov UI iz Priloge III, točka 2, na trg ali v uporabo ponudnik ali, kadar je to ustrezno, pooblaščen zastopnik sebe in svoj sistem registrira v podatkovni zbirki EU iz člena 71.

2. Pred dajanjem sistema UI, za katerega je ponudnik ugotovil, da v skladu s členom 6(3) ne šteje za visokotvegan, na trg ali v uporabo ponudnik ali, kadar je to ustrezno, pooblaščen zastopnik sebe in navedeni sistem registrira v podatkovni zbirki EU iz člena 71.
3. Pred dajanjem v uporabo ali pred uporabo visokotveganega sistema UI iz Priloge III, z izjemo visokotveganih sistemov UI iz Priloge III, točka 2, se uvajalci, ki so javni organi, institucije, organi, uradi ali agencije Unije ali osebe, ki delujejo v njihovem imenu, registrirajo, izberejo sistem in registrirajo njegovo uporabo v podatkovni zbirki EU iz člena 71.
4. Za visokotvegane sisteme UI iz Priloge III, točke 1, 6 in 7, na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja se registracija iz odstavkov 1, 2 in 3 tega člena izvede v varnem nejavnem delu podatkovne zbirke EU iz člena 71 in vključuje le naslednje informacije, kot je ustrezno, iz:
 - (a) Priloge VIII, oddelek A, točke 1 do 10, razen točk 6, 8 in 9;
 - (b) Priloge VIII, oddelek B, točke 1 do 5 ter točki 8 in 9;
 - (c) Priloge VIII, oddelek C, točke 1 do 3;
 - (d) Priloge IX, točke 1, 2, 3 in 5.

Dostop do ustreznih omejenih delov podatkovne zbirke EU iz prvega pododstavka tega odstavka imajo samo Komisija in nacionalni organi iz člena 74(8).

5. Visokotvegani sistemi UI iz Priloge III, točka 2, se registrirajo na nacionalni ravni.

Poglavje IV

Obveznosti ponudnikov in uvajalcev nekaterih sistemov UI glede preglednosti

Člen 50

Obveznosti ponudnikov in uvajalcev nekaterih sistemov UI glede preglednosti

1. Ponudniki zagotovijo, da so sistemi UI, namenjeni neposredni interakciji s fizičnimi osebami, zasnovani in razviti tako, da so zadevne fizične osebe obveščene, da so v interakciji s sistemom UI, razen če je to očitno z vidika razmeroma dobro obveščene, pozorne in preudarne fizične osebe ob upoštevanju okoliščin in konteksta uporabe. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb ne uporablja za sisteme UI, ki so z zakonom odobreni za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj, razen če so ti sistemi na voljo javnosti za prijavo kaznivega dejanja.

2. Ponudniki sistemov UI, vključno s sistemi UI za splošne namene, ki ustvarjajo sintetično zvočno, slikovno, video ali besedilno vsebino, zagotovijo, da so izhodni podatki sistema UI označeni v strojno berljivi obliki in jih je mogoče prepoznati kot umetno ustvarjene ali prirejene. Ponudniki zagotovijo, da so njihove tehnične rešitve učinkovite, interoperabilne, robustne in zanesljive, kolikor je to tehnično izvedljivo, pri čemer upoštevajo posebnosti in omejitve različnih vrst vsebin, stroške izvajanja in splošno priznane najsodobnejše tehnološke dosežke, kar se lahko odraža v ustreznih tehničnih standardih. Ta obveznost se ne uporablja, kolikor sistemi UI zagotavljajo podporno funkcijo za standardno urejanje ali ne spreminjajo bistveno vhodnih podatkov, ki jih zagotovi uvajalec, ali njihove semantike ali kadar so z zakonom dovoljeni za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj.
3. Uvajalci sistema za prepoznavanje čustev ali sistema za biometrično kategorizacijo o delovanju sistema obvestijo fizične osebe, ki so mu izpostavljene, in obdelujejo osebne podatke v skladu z uredbama (EU) 2016/679 in (EU) 2018/1725 ter Direktivo (EU) 2016/680, kot je ustrezno. Ta obveznost se ob upoštevanju ustreznih zaščitnih ukrepov za pravice in svoboščine tretjih oseb ter v skladu s pravom Unije ne uporablja za sisteme UI, ki se uporabljajo za biometrično kategorizacijo in prepoznavanje čustev ter so z zakonom dovoljeni za odkrivanje, preprečevanje ali preiskovanje kaznivih dejanj.

4. Uvajalci sistema UI, ki ustvarja ali prireja slikovno, zvočno ali video vsebino, ki je globoki ponaredek, morajo razkriti, da je bila vsebina umetno ustvarjena ali prirejena. Ta obveznost se ne uporablja, kadar je uporaba zakonsko dovoljena za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj. Kadar je vsebina del očitno umetniškega, ustvarjalnega, satiričnega, fiktivnega ali podobnega dela ali programa, so obveznosti glede preglednosti iz tega odstavka omejene na razkritje obstoja take ustvarjene ali prirejene vsebine na ustrezen način, ki ne ovira prikazovanja ali uživanja dela.

Uvajalci sistema UI, ki ustvarja ali prireja besedilo, ki se objavi z namenom obveščanja javnosti o zadevah javnega interesa, morajo razkriti, da je bilo besedilo umetno ustvarjeno ali prirejeno. Ta obveznost se ne uporablja, kadar je uporaba zakonsko dovoljena za odkrivanje, preprečevanje, preiskovanje ali pregon kaznivih dejanj ali kadar je bila vsebina, ustvarjena z UI, predmet človeške preverbe ali uredniškega pregleda in kadar ima fizična ali pravna oseba uredniško odgovornost za objavo vsebine.

5. Informacije iz odstavkov 1 do 4 se dajo na voljo zadevnim fizičnim osebam na jasn in razpoznaven način ter najpozneje ob prvi interakciji ali izpostavljenosti. Informacije morajo biti skladne z veljavnimi zahtevami glede dostopnosti.
6. Odstavki 1 do 4 ne vplivajo na zahteve in obveznosti iz poglavja III in ne posegajo v druge obveznosti glede preglednosti, ki so za uvajalce sistemov UI določene v pravu Unije ali nacionalnem pravu.

7. Urad za UI spodbuja in olajšuje pripravo kodeksov prakse na ravni Unije, da se omogoči učinkovito izvajanje obveznosti glede odkrivanja in označevanja umetno ustvarjenih ali prirejenih vsebin. Komisija lahko sprejme izvedbene akte za odobritev teh kodeksov prakse v skladu s postopkom iz člena 56(6). Če meni, da kodeks ni ustrezen, lahko Komisija sprejme izvedbeni akt, s katerim določi skupna pravila za izvajanje navedenih obveznosti v skladu s postopkom pregleda iz člena 98(2).

Poglavje V

Modeli UI za splošne namene

ODDELEK 1

PRAVILA ZA RAZVRŠČANJE

Člen 51

Razvrstitev modelov UI za splošne namene kot modelov UI za splošne namene s sistemskim tveganjem

1. Model UI za splošne namene se razvrsti kot model UI za splošne namene s sistemskim tveganjem, če izpolnjuje katerega od naslednjih pogojev:
 - (a) ima zmogljivosti z visoko učinkovitostjo, ocenjene na podlagi ustreznih tehničnih orodij in metodologij, vključno s kazalniki in merili uspešnosti;

- (b) ima zmogljivosti ali učinek, ki so enakovredni tistim iz točke (a), ob upoštevanju meril iz Priloge XIII, na podlagi odločitve Komisije, in sicer po uradni dolžnosti ali na podlagi kvalificiranega opozorila znanstvenega odbora.
2. Za model UI za splošne namene se predpostavlja, da ima zmogljivosti z visoko učinkovitostjo na podlagi odstavka 1, točka (a), kadar je skupna količina izračuna, uporabljena za njegovo učenje, merjeno z operacijami s plavajočo vejico, večja od 10^{25} .
3. Komisija sprejme delegirane akte v skladu s členom 97 za spremembo pragov iz odstavkov 1 in 2 tega člena ter dopolnitev meril uspešnosti in kazalnikov glede na tehnološki razvoj, ki zadeva na primer algoritemsko izboljšave ali večjo učinkovitost strojne opreme, kadar je to potrebno, da bi bili v teh pragovih upoštevani najsodobnejši tehnološki dosežki.

Člen 52

Postopek

1. Kadar model UI za splošne namene izpolnjuje pogoj iz člena 51(1), točka (a), zadevni ponudnik o tem nemudoma, v vsakem primeru pa v dveh tednih po izpolnitvi te zahteve ali po tem, ko je znano, da bo izpolnjena, uradno obvesti Komisijo. To uradno obvestilo vključuje informacije, iz katerih je razvidno, da je ustrezna zahteva izpolnjena. Če Komisija ugotovi, da model UI za splošne namene predstavlja sistemska tveganja, o katerih ni bila uradno obveščena, se lahko odloči, da ga bo označila za model s sistemskim tveganjem.

2. Ponudnik modela UI za splošne namene, ki izpolnjuje pogoj iz člena 51(1), točka (a), lahko ob uradnem obvestilu predloži dovolj utemeljene argumente, s katerimi dokaže, da model UI za splošne namene izjemoma, čeprav izpolnjuje navedeno zahtevo, zaradi svojih posebnih značilnosti ne predstavlja sistemskih tveganj in zato ne bi smel biti razvrščen kot model UI za splošne namene s sistemskim tveganjem.
3. Kadar Komisija ugotovi, da argumenti, predloženi na podlagi odstavka 2, niso dovolj utemeljeni in da zadevni ponudnik ni mogel dokazati, da model UI za splošne namene zaradi svojih posebnih značilnosti ne predstavlja sistemskih tveganj, te argumente zavrne, model UI za splošne namene pa se šteje za model UI za splošne namene s sistemskim tveganjem.
4. Komisija lahko na podlagi meril iz Priloge XIII po uradni dolžnosti ali na podlagi kvalificiranega opozorila znanstvenega odbora na podlagi člena 90(1), točka (a), model UI za splošne namene označi za model, ki predstavlja sistemska tveganja.

Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, da spremeni Prilogo XIII, s tem da določi in posodobi merila iz navedene priloge.

5. Komisija na obrazloženo zahtevo ponudnika, katerega model je bil označen za model UI za splošne namene s sistemskim tveganjem na podlagi odstavka 4, upošteva zahtevo in se lahko odloči, da ponovno oceni, ali se lahko za model UI za splošne namene še vedno šteje, da predstavlja sistemska tveganja na podlagi meril iz Priloge XIII. Taka zahteva vsebuje objektivne, podrobne in nove razloge, ki so se pojavili po odločitvi glede označitve. Ponudniki ponovne ocene ne morejo zahtevati prej kot šest mesecev po odločitvi glede označitve. Kadar se Komisija po ponovni oceni odloči, da bo ohranila označitev modela UI za splošne namene s sistemskim tveganjem, ponudniki ponovne zahteve ne morejo zahtevati prej kot šest mesecev po tej odločitvi.
6. Komisija zagotovi objavo seznama modelov UI za splošne namene s sistemskim tveganjem in ga posodablja, ne da bi pri tem posegala v potrebo po spoštovanju in varstvu pravic intelektualne lastnine in zaupnih poslovnih informacij ali poslovnih skrivnosti v skladu s pravom Unije in nacionalnim pravom.

ODDELEK 2

OBVEZNOSTI, NALOŽENE PONUDNIKOM MODELOV UI ZA SPLOŠNE NAMENE

Člen 53

Obveznosti, naložene ponudnikom modelov UI za splošne namene

1. Ponudniki modelov UI za splošne namene:
 - (a) pripravijo in posodablajo tehnično dokumentacijo modela, vključno s postopkom učenja in testiranja ter rezultati njegovega ocenjevanja, ki vsebuje vsaj informacije iz Priloge XI, da se na zahtevo predloži Uradu za UI in pristojnim nacionalnim organom;
 - (b) pripravijo, posodablajo in dajejo na voljo informacije in dokumentacijo za ponudnike sistemov UI, ki nameravajo model UI za splošne namene integrirati v svoje sisteme UI. Brez poseganja v potrebo po spoštovanju in varstvu pravic intelektualne lastnine in zaupnih poslovnih informacij ali poslovnih skrivnosti v skladu s pravom Unije in nacionalnim pravom informacije in dokumentacija:
 - (i) ponudnikom sistemov UI omogočajo, da dobro razumejo zmogljivosti in omejitve modela UI za splošne namene ter izpolnjujejo svoje obveznosti na podlagi te uredbe, ter
 - (ii) vsebujejo vsaj elemente iz Priloge XII;

- (c) vzpostavijo politiko za doseganje skladnosti s pravom Unije o avtorskih in sorodnih pravicah, zlasti za opredelitev in spoštovanje, tudi z najsodobnejšimi tehnologijami, pridržanj pravic, izraženih na podlagi člena 4(3) Direktive (EU) 2019/790;
 - (d) v skladu s predlogo, ki jo zagotovi Urad za UI, pripravijo in objavijo dovolj podroben povzetek vsebine, ki se uporablja za učenje modela UI za splošne namene.
2. Obveznosti iz odstavka 1, točki (a) in (b), ne veljajo za ponudnike modelov UI, ki so bili objavljeni na podlagi proste in odprtokodne licence, ki omogoča dostop do modela, njegovo uporabo, spreminjanje in distribucijo ter katere parametri, vključno z utežmi, informacijami o strukturi modela in informacijami o uporabi modela, so javno dostopni. Ta izjema se ne uporablja za modele UI za splošne namene s sistemskimi tveganji.
3. Ponudniki modelov UI za splošne namene pri izvajanju svojih pristojnosti in pooblastil na podlagi te uredbe po potrebi sodelujejo s Komisijo in pristojnimi nacionalnimi organi.

4. Ponudniki modelov UI za splošne namene se lahko do objave harmoniziranega standarda zanašajo na kodekse prakse v smislu člena 56, da dokažejo skladnost z obveznostmi iz odstavka 1 tega člena. Izpolnjevanje evropskih harmoniziranih standardov zagotavlja ponudnikom domnevo o skladnosti, kadar ti standardi zajemajo te obveznosti. Ponudniki modelov UI za splošne namene, ki ne upoštevajo odobrenega kodeksa prakse ali ne izpolnjujejo evropskega harmoniziranega standarda, dokažejo, da imajo druge ustrezne načine za zagotavljanje skladnosti, ki jih oceni Komisija.
5. Da se olajša skladnost s Prilogo XI, zlasti s točko 2(d) in (e) navedene priloge, se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97, v katerih se podrobno opredelijo metodologije merjenja in izračunavanja, da se omogoči primerljiva in preverljiva dokumentacija.
6. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 97(2) za spremembo prilog XI in XII glede na hiter tehnološki razvoj.
7. Vse informacije ali dokumentacija, pridobljene na podlagi tega člena, vključno s poslovnimi skrivnostmi, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 54

Pooblašчени zastopniki ponudnikov modelov UI za splošne namene

1. Ponudniki s sedežem v tretji državi pred dajanjem modela UI za splošne namene na trg Unije s pisnim pooblastilom imenujejo pooblaščenega zastopnika s sedežem v Uniji.

2. Ponudnik svojemu pooblaščenemu zastopniku omogoči, da opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika.
3. Pooblaščen zastopnik opravlja naloge, določene v pooblastilu, ki ga prejme od ponudnika. Uradu za UI na njegovo zahtevo predloži izvod pooblastila, in sicer v enem od uradnih jezikov institucij Unije. Za namene te uredbe pooblastilo pooblaščenemu zastopniku omogoča, da opravlja naslednje naloge:
 - (a) preveri, ali je bila tehnična dokumentacija, določena v Prilogi XI, pripravljena in ali je ponudnik izpolnil vse obveznosti iz člena 53 in, kadar je ustrezno, člena 55;
 - (b) hrani izvod tehnične dokumentacije, določene v Prilogi XI, da je za obdobje 10 let po tem, ko je bil model UI za splošne namene dan na trg, na voljo Uradu za UI in pristojnim nacionalnim organom, ter kontaktne podatke ponudnika, ki je imenoval pooblaščenega zastopnika;
 - (c) Uradu za UI na obrazloženo zahtevo zagotovi vse informacije in dokumentacijo, vključno s tistimi iz točke (b), s katerimi dokaže, da izpolnjuje obveznosti iz tega poglavja;
 - (d) na obrazloženo zahtevo sodeluje z Uradom za UI in pristojnimi nacionalnimi organi pri vseh ukrepih, ki jih slednji sprejmejo v zvezi z modelom UI za splošne namene s sistemskimi tveganji, tudi kadar je model vključen v sisteme UI, dane na trg ali v uporabo v Uniji.

4. Na podlagi pooblastila je pooblaščen zastopnik pooblaščen, da lahko Urad za UI ali pristojni organi nanj, poleg ponudnika ali namesto njega, naslovijo vsa vprašanja, povezana z zagotavljanjem skladnosti s to uredbo.
5. Pooblaščen zastopnik odpove pooblastilo, če meni ali utemeljeno domneva, da ponudnik ravna v nasprotju s svojimi obveznostmi na podlagi te uredbe. V takem primeru tudi nemudoma obvesti Urad za UI o odpovedi pooblastila in o razlogih zanjo.
6. Obveznost iz tega člena ne velja za ponudnike modelov UI za splošne namene, ki so bili objavljeni na podlagi proste in odprtokodne licence, ki omogoča dostop do modela, njegovo uporabo, spreminjanje in distribucijo ter katere parametri, vključno z utežmi, informacijami o strukturi modela in informacijami o uporabi modela, so javno dostopni, razen če modeli UI za splošne namene predstavljajo sistemska tveganja.

ODDELEK 3
OBVEZNOSTI PONUDNIKOV MODELOV UI ZA SPLOŠNE NAMENE
S SISTEMSKIM TVEGANJEM

Člen 55

Obveznosti ponudnikov modelov UI za splošne namene s sistemskim tveganjem

1. Poleg obveznosti iz členov 53 in 54 ponudniki modelov UI za splošne namene s sistemskim tveganjem:
 - (a) izvedejo ocene modelov v skladu s standardiziranimi protokoli in orodji, ki upoštevajo najsodobnejše tehnološke dosežke, vključno z izvajanjem in dokumentiranjem testiranja modelov po načelu kontradiktornosti z namenom prepoznavanja in zmanjšanja sistemskega tveganja;
 - (b) ocenijo in zmanjšajo morebitna sistemska tveganja na ravni Unije, vključno z njihovimi viri, ki lahko izhajajo iz razvoja, dajanja na trg ali uporabe modelov UI za splošne namene s sistemskim tveganjem;
 - (c) spremljajo in dokumentirajo resne incidente ter informacije o njih in morebitne popravne ukrepe za njihovo odpravo brez nepotrebnega odlašanja sporočajo Uradu za UI in po potrebi pristojnim nacionalnim organom;
 - (d) zagotavljajo ustrezno raven kibernetске zaščite za model UI za splošne namene s sistemskim tveganjem in fizično infrastrukturo modela.

2. Ponudniki modelov UI za splošne namene s sistemskim tveganjem se lahko do objave harmoniziranega standarda zanašajo na kodekse prakse v smislu člena 56, da dokažejo skladnost z obveznostmi iz odstavka 1 tega člena. Izpolnjevanje evropskih harmoniziranih standardov zagotavlja ponudnikom domnevo o skladnosti, kadar ti standardi zajemajo te obveznosti. Ponudniki modelov UI za splošne namene s sistemskim tveganjem, ki ne upoštevajo odobrenega kodeksa prakse ali ne izpolnjujejo evropskega harmoniziranega standarda, dokažejo, da imajo druge ustrezne načine za zagotavljanje skladnosti, ki jih oceni Komisija.
3. Vse informacije ali dokumentacija, pridobljene na podlagi tega člena, vključno s poslovnimi skrivnostmi, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

ODDELEK 4

KODEKSI PRAKSE

Člen 56

Kodeksi prakse

1. Urad za UI spodbuja in olajšuje pripravo kodeksov prakse na ravni Unije, da bi prispeval k pravilni uporabi te uredbe ob upoštevanju mednarodnih pristopov.

2. Urad za UI in Odbor si prizadevata zagotoviti, da kodeksi prakse zajemajo vsaj obveznosti iz členov 53 in 55, vključno z naslednjimi elementi:
- (a) načini za zagotavljanje, da se informacije iz člena 53(1), točki (a) in (b), posodablajo glede na tržni in tehnološki razvoj;
 - (b) ustrezno ravno podrobnosti za povzetek o vsebini, ki se uporablja za učenje;
 - (c) opredelitvijo vrste in narave sistemskih tveganj na ravni Unije, po potrebi vključno z njihovimi viri;
 - (d) ukrepi, postopki in načini za oceno in obvladovanje sistemskih tveganj na ravni Unije, vključno s pripadajočo dokumentacijo, ki so sorazmerni s tveganji, upoštevajo njihovo resnost in verjetnost ter upoštevajo posebne izzive pri obvladovanju teh tveganj glede na možne načine, na katere se lahko taka tveganja pojavijo in udejanijo vzdolž verige vrednosti UI.
3. Urad za UI lahko k sodelovanju pri pripravi kodeksov prakse povabi vse ponudnike modelov UI za splošne namene in ustrezne pristojne nacionalne organe. V procesu lahko sodelujejo organizacije civilne družbe, industrija, akademski krogi in drugi ustrezni deležniki, kot so ponudniki nižje v verigi in neodvisni strokovnjaki.

4. Urad za UI in Odbor si prizadevata zagotoviti, da kodeksi prakse jasno določajo njune posebne cilje in vsebujejo zaveze ali ukrepe, po potrebi tudi ključne kazalnike uspešnosti, da se zagotovi doseganje teh ciljev, ter da so v njih ustrezno upoštevani potrebe in interesi vseh zainteresiranih strani na ravni Unije, tudi oseb, ki jih to zadeva.
5. Urad za UI si prizadeva zagotoviti, da mu sodelujoči pri kodeksu prakse redno poročajo o uresničevanju zavez in sprejetih ukrepov ter posledičnih rezultatih, po potrebi tudi glede na ključne kazalnike uspešnosti. V ključnih kazalnikih uspešnosti in obveznostih poročanja se odražajo razlike v velikosti in zmogljivosti različnih sodelujočih.
6. Urad za UI in Odbor redno spremljata in ocenjujeta, kako sodelujoči dosegajo cilje kodeksov prakse in kako prispevajo k pravilni uporabi te uredbe. Urad za UI in Odbor ocenita, ali kodeksi prakse zajemajo obveznosti iz členov 53 in 55, ter redno spremljata in ocenjujeta doseganje ciljev v zvezi s tem. Svojo oceno ustreznosti kodeksov prakse objavita.

Komisija lahko z izvedbenim aktom odobri kodeks prakse in mu da splošno veljavnost v Uniji. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).

7. Urad za UI lahko povabi vse ponudnike modelov UI za splošne namene, da pristopijo h kodeksom prakse. Za ponudnike modelov UI za splošne namene, ki ne predstavljajo sistemskih tveganj, je pristop lahko omejen na obveznosti iz člena 53, razen če izrecno izrazijo svoj interes za pristop k celotnemu kodeksu.
8. Urad za UI po potrebi spodbuja in olajšuje pregled in prilagoditev kodeksov prakse, zlasti glede na nastajajoče standarde. Urad za UI pomaga ocenjevati razpoložljive standarde.
9. Kodeksi prakse se pripravijo najpozneje do... [devet mesecev od datuma začetka veljavnosti te uredbe]. Urad za UI sprejme potrebne ukrepe, vključno s povabilom ponudnikom na podlagi odstavka 7.

Če kodeksa prakse do ... [12 mesecev od datuma začetka veljavnosti] ni mogoče dokončati ali če Urad za UI na podlagi svoje ocene na podlagi odstavka 6 tega člena meni, da ni ustrezen, lahko Komisija z izvedbenimi akti določi skupna pravila za izvajanje obveznosti iz členov 53 in 55, vključno z elementi iz odstavka 2 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

Poglavje VI

Ukrepi v podporo inovacijam

Člen 57

Regulativni peskovniki za UI

1. Države članice zagotovijo, da njihovi pristojni organi na nacionalni ravni vzpostavijo vsaj en regulativni peskovnik za UI, ki začne delovati najpozneje ... [24 mesecev od datuma začetka veljavnosti te uredbe]. Ta peskovnik se lahko vzpostavi skupaj s pristojnimi organi drugih držav članic. Komisija lahko za vzpostavitev in delovanje regulativnih peskovnikov za UI zagotovi tehnično podporo, svetovanje in orodja.

Obveznost iz prvega pododstavka se lahko izpolni tudi s sodelovanjem v obstoječem peskovniku, če tako sodelovanje zagotavlja enakovredno nacionalno zastopanost sodelujočih držav članic.

2. Na regionalni ali lokalni ravni ali skupaj s pristojnimi organi drugih držav članic se lahko vzpostavijo tudi dodatni regulativni peskovniki za UI.
3. Evropski nadzornik za varstvo podatkov lahko vzpostavi tudi regulativni peskovnik za UI za institucije, organe, urade in agencije Unije ter lahko opravlja vloge in naloge pristojnih nacionalnih organov v skladu s tem poglavjem.

4. Države članice zagotovijo, da pristojni organi iz odstavkov 1 in 2 dodelijo zadostna sredstva za učinkovito in pravočasno izpolnjevanje tega člena. Kadar je primerno, pristojni nacionalni organi sodelujejo z drugimi ustreznimi organi in lahko dopustijo udeležnost drugih akterjev ekosistema UI. Ta člen ne vpliva na druge regulativne peskovnike, vzpostavljene na podlagi prava Unije ali nacionalnega prava. Države članice zagotovijo ustrezno raven sodelovanja med organi, ki nadzorujejo te druge peskovnike, in pristojnimi nacionalnimi organi.
5. Regulativni peskovniki za UI, vzpostavljeni na podlagi odstavka 1, zagotavljajo nadzorovano okolje, ki spodbuja inovacije ter omogoča razvoj, učenje, testiranje in validacijo inovativnih sistemov UI za določen čas, preden se dajo na trg ali v uporabo, v skladu s posebnim načrtom peskovnika, o katerem se dogovorijo ponudniki ali potencialni ponudniki in pristojni organ. Taki peskovniki lahko vključujejo testiranje v realnih razmerah, ki se v njih nadzoruje.
6. Pristojni organi v regulativnem peskovniku za UI po potrebi zagotovijo smernice, nadzor in podporo, kar zadeva opredeljevanje tveganja – zlasti za temeljne pravice, zdravje in varnost –, testiranje, ukrepe za zmanjšanje tveganj in njihovo učinkovitost glede na obveznosti in zahteve iz te uredbe ter po potrebi iz drugega prava Unije in nacionalnega prava, katerih upoštevanje se nadzoruje v peskovniku.
7. Pristojni organi ponudnikom in potencialnim ponudnikom, ki sodelujejo v regulativnem peskovniku za UI, zagotovijo smernice o regulativnih pričakovanjih ter o tem, kako izpolniti zahteve in obveznosti iz te uredbe.

Pristojni organ na zahtevo ponudnika ali potencialnega ponudnika sistema UI predloži pisno dokazilo o dejavnostih, ki so bile uspešno izvedene v peskovniku. Predloži tudi poročilo o izstopu, v katerem podrobno opiše dejavnosti, izvedene v peskovniku, ter povezane rezultate in učne izide. Ponudniki lahko tako dokumentacijo uporabijo za to, da s postopkom ugotavljanja skladnosti ali z ustreznimi dejavnostmi nadzora trga dokažejo skladnost s to uredbo. V zvezi s tem organi za nadzor trga in priglašeni organi pozitivno upoštevajo poročila o izstopu in pisna dokazila, ki jih predloži pristojni nacionalni organ, da bi v razumni meri pospešili postopke ugotavljanja skladnosti.

8. Komisija in Odbor sta ob upoštevanju določb o zaupnosti iz člena 78 in s soglasjem ponudnika ali potencialnega ponudnika pooblaščen za dostop do poročil o izstopu in jih, če je to primerno, upoštevata pri izvajanju svojih nalog na podlagi te uredbe. Če se ponudnik ali potencialni ponudnik in pristojni nacionalni organ izrecno strinjata, se lahko poročilo o izstopu objavi na enotni informacijski platformi iz tega člena.
9. Namen vzpostavitve regulativnih peskovnikov za UI je prispevati k naslednjim ciljem:
 - (a) izboljšanju pravne varnosti, da se doseže regulativna skladnost s to uredbo ali po potrebi z drugim veljavnim pravom Unije in nacionalnim pravom;
 - (b) podpiranju izmenjave najboljših praks s sodelovanjem z organi, vključenimi v regulativni peskovnik za UI;

- (c) spodbujanju inovacij in konkurenčnosti ter olajšanju razvoja ekosistema UI;
 - (d) prispevanju k regulativnemu učenju, ki temelji na dokazih;
 - (e) olajšanju in pospežitvi dostopa sistemov UI do trga Unije, zlasti če so njihovi ponudniki MSP, vključno z zagonskimi podjetji.
10. Če inovativni sistemi UI vključujejo obdelavo osebnih podatkov ali kako drugače spadajo v nadzorno pristojnost drugih nacionalnih organov ali pristojnih organov, ki zagotavljajo ali podpirajo dostop do podatkov, nacionalni pristojni organi zagotovijo, da so nacionalni organi za varstvo podatkov in ti drugi nacionalni ali pristojni organi povezani z delovanjem regulativnega peskovnika za UI in vključeni v nadzor omenjenih vidikov v okviru svojih nalog in pooblastil.
11. Regulativni peskovniki za UI ne vplivajo na pooblastila pristojnih organov, ki nadzirajo peskovnike, za nadzor ali popravne ukrepe, tudi na regionalni ali lokalni ravni ne. Vsa pomembna tveganja za zdravje in varnost ter temeljne pravice, prepoznana med razvojem in testiranjem takih sistemov UI, se ustrezno zmanjšajo. Nacionalni pristojni organi so pooblaščen, da začasno ali trajno prekinejo postopek testiranja ali sodelovanje v peskovniku, če tveganj ni mogoče učinkovito zmanjšati, in o taki odločitvi obvestijo Urad za UI. Nacionalni pristojni organi svoja nadzorna pooblastila izvajajo v mejah ustreznega prava in pri izvajanju pravnih določb v zvezi z določenim projektom peskovnika za UI uporabljajo svoja diskrecijska pooblastila, da bi podprli inovacije na področju UI v Uniji.

12. Ponudniki in potencialni ponudniki, ki sodelujejo v regulativnem peskovniku za UI, so na podlagi veljavnega prava Unije in nacionalnega prava o odgovornosti še naprej odgovorni za škodo, povzročeno tretjim osebam zaradi eksperimentov, ki se izvajajo v peskovniku. Kadar pa potencialni ponudniki spoštujejo posebni načrt in pogoje za sodelovanje ter v dobri veri sledijo smernicam nacionalnih pristojnih organov, organi ne naložijo upravnih kazni za kršitev te uredbe. Kadar so bili v nadzor sistema UI v peskovniku dejavno vključeni drugi pristojni organi, odgovorni za drugo pravo Unije in nacionalno pravo, in so zagotovili smernice za skladnost, se v zvezi s tem pravom ne naložijo upravne kazni.
13. Regulativni peskovniki za UI so zasnovani in se izvajajo tako, da po potrebi olajšujejo čezmejno sodelovanje med pristojnimi nacionalnimi organi.
14. Nacionalni pristojni organi usklajujejo svoje dejavnosti in sodelujejo v okviru Odbora.
15. Pristojni nacionalni organi o vzpostavitvi peskovnika obvestijo Urad za UI in Odbor ter ju lahko zaprosijo za podporo in smernice. Urad za UI objavi seznam načrtovanih in obstoječih peskovnikov ter ga posodablja, da bi spodbudil večjo interakcijo v regulativnih peskovnikih za UI in čezmejno sodelovanje.

16. Pristojni nacionalni organi Uradu za UI in Odboru predložijo letna poročila, najprej eno leto po vzpostavitvi regulativnega peskovnika za UI, nato pa vsako leto do njegove ukinitve, tako kot tudi končno poročilo. Ta poročila vsebujejo informacije o napredku in rezultatih izvajanja teh peskovnikov, vključno z najboljšimi praksami, incidenti, pridobljenimi izkušnjami in priporočili o njihovi vzpostavitvi ter po potrebi o uporabi in morebitni reviziji te uredbe, vključno s povezanimi delegiranimi in izvedbenimi akti, in o uporabi drugega prava Unije, ki ga v peskovniku nadzorujejo pristojni organi. Pristojni nacionalni organi ta letna poročila ali njihove povzetke objavijo na spletu. Komisija pri izvajanju svojih nalog na podlagi te uredbe, kadar je primerno, upošteva ta letna poročila.
17. Komisija razvije enotni in namenski vmesnik, ki vsebuje vse ustrezne informacije v zvezi z regulativnimi peskovniki za UI, da bi lahko deležniki vstopali v interakcijo z regulativnimi peskovniki za UI in vlagali poizvedbe pri pristojnih organih ter zaprošali za nezavezujoče smernice glede skladnosti inovativnih proizvodov, storitev in poslovnih modelov, ki vključujejo tehnologije UI, v skladu s členom 62(1), točka (c). Komisija se po potrebi proaktivno usklajuje s pristojnimi nacionalnimi organi.

Člen 58

Podrobnosti v zvezi z regulativnimi peskovniki za UI in njihovo delovanje

1. Da bi se izognili razdrobljenosti po Uniji, Komisija sprejme izvedbene akte, v katerih določi podrobnosti za vzpostavitev, razvoj, izvajanje, delovanje in nadzor regulativnih peskovnikov za UI. Ti izvedbeni akti med drugim vsebujejo skupna načela o naslednjih elementih:
 - (a) merilih za upravičenost in izbor za sodelovanje v regulativnem peskovniku za UI;
 - (b) postopkih za vlogo, sodelovanje, spremljanje, izstop iz regulativnega peskovnika za UI in njegovo prenehanje, vključno z načrtom peskovnika in poročilom o izstopu;
 - (c) pogojih, ki veljajo za udeležence.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).
2. Z izvedbenim aktom iz odstavka 1 se zagotovi:
 - (a) da so regulativni peskovniki za UI odprti za vse ponudnike in potencialne ponudnike sistema UI, ki izpolnjujejo pregledna in pravična merila za upravičenost in izbor, in da pristojni nacionalni organi vlagatelje obvestijo o svoji odločitvi v treh mesecih od vložitve vloge;

- (b) da regulativni peskovniki za UI omogočajo širok in enak dostop ter sledijo povpraševanju po sodelovanju; ponudniki ali potencialni ponudniki lahko vloge predložijo tudi v partnerstvih z uvajalci in drugimi ustreznimi tretjimi osebami;
- (c) da se s podrobnostmi in pogoji v zvezi z regulativnimi peskovniki za UI v največji možni meri podpira prožnost, ki pristojnim nacionalnim organom omogoča vzpostavitev in upravljanje njihovih regulativnih peskovnikov za UI;
- (d) da je dostop do regulativnih peskovnikov za UI za MSP, vključno z zagonskimi podjetji, brezplačen, brez poseganja v izredne stroške, ki jih lahko pristojni nacionalni organi izterjajo na pošten in sorazmeren način;
- (e) da se ponudnikom ali potencialnim ponudnikom z učnimi izidi regulativnih peskovnikov za UI pomaga pri izpolnjevanju obveznosti glede ugotavljanja skladnosti iz te uredbe in prostovoljni uporabi kodeksov ravnanja iz člena 95;
- (f) da regulativni peskovniki za UI olajšujejo vključevanje drugih ustreznih akterjev v ekosistem UI, na primer priglašeni organov in organizacij za standardizacijo, MSP, vključno z zagonskimi podjetji, podjetij, inovatorjev, centrov za testiranje in eksperimentiranje, raziskovalnih in eksperimentalnih laboratorijev ter evropskih vozlišč za digitalne inovacije, centrov odličnosti, posameznih raziskovalcev, da bi omogočili in olajšali sodelovanje z javnim in zasebnimi sektorji;

- (g) da so postopki, procesi in upravne zahteve za vlogo, izbiro, sodelovanje in izstop iz regulativnega peskovnika za UI preprosti, lahko razumljivi in jasno predstavljeni, da bi olajšali udeležbo MSP, vključno z zagonskimi podjetji, z omejenimi pravnimi in upravnimi zmogljivostmi, ter da so racionalizirani po vsej Uniji, da bi preprečili razdrobljenost in da bi bila udeležba v regulativnem peskovniku za UI, ki ga vzpostavi država članica ali evropski nadzornik za varstvo podatkov, vzajemno in enotno priznana ter da bi imela enake pravne učinke po vsej Uniji;
- (h) da je sodelovanje v regulativnem peskovniku za UI omejeno na obdobje, ki je primerno glede na kompleksnost in obseg projekta in ki ga lahko pristojni nacionalni organ podaljša;
- (i) da regulativni peskovniki za UI olajšujejo razvoj orodij in infrastrukture za testiranje, primerjalno analizo, ocenjevanje in razlago razsežnosti sistemov UI, ki so pomembne za regulativno učenje, na primer točnosti, robustnosti in kibernetске varnosti, pa tudi ukrepov za zmanjšanje tveganj, kar zadeva temeljne pravice in družbo na splošno.

3. Potencialni ponudniki v regulativnih peskovnikih za UI, zlasti MSP in zagonska podjetja, so po potrebi usmerjeni k storitvam pred uvedbo, kot so smernice o izvajanju te uredbe, k drugim storitvam z dodano vrednostjo, kot so pomoč pri dokumentih za standardizacijo in certificiranju, centri za testiranje in eksperimentiranje, evropska vozlišča za digitalne inovacije in centri odličnosti.

4. Kadar pristojni nacionalni organi presoja o odobritvi testiranja v realnih razmerah, ki se nadzoruje v okviru regulativnega peskovnika za UI, ki se vzpostavi na podlagi tega člena, se z udeleženci izrecno dogovorijo o pogojih takega testiranja in zlasti o ustreznih zaščitnih ukrepih za varovanje temeljnih pravic, zdravja in varnosti. Kadar je primerno, sodelujejo z drugimi pristojnimi nacionalnimi organi, da bi zagotovili dosledne prakse po vsej Uniji.

Člen 59

Nadaljnja obdelava osebnih podatkov za razvoj določenih sistemov UI v javnem interesu v regulativnem peskovniku za UI

1. V regulativnem peskovniku za UI se osebni podatki, zakonito zbrani za druge namene, lahko obdelujejo izključno za namene razvoja, učenja in testiranja nekaterih sistemov UI v peskovniku, če so izpolnjeni vsi naslednji pogoji:
- (a) javni organ ali druga fizična ali pravna oseba razvije sisteme UI za zaščito bistvenega javnega interesa na enem ali več naslednjih področjih:
 - (i) javna varnost in javno zdravje, vključno z odkrivanjem, diagnosticiranjem, preprečevanjem, obvladovanjem in zdravljenjem bolezni ter izboljšanjem sistemov zdravstvenega varstva;
 - (ii) visoka raven varstva in izboljšanje kakovosti okolja, ohranjanje biotske raznovrstnosti, varstvo pred onesnaževanjem, ukrepi za zeleni prehod ter blažitev podnebnih sprememb in prilagajanje nanje;

- (iii) trajnostna energija;
 - (iv) varnost in odpornost prometnih sistemov in mobilnosti, kritične infrastrukture in omrežij;
 - (v) učinkovitost in kakovost javne uprave in javnih storitev;
- (b) obdelani podatki so potrebni za izpolnjevanje ene ali več zahtev iz poglavja III, oddelek 2, kadar teh zahtev ni mogoče učinkovito izpolniti z obdelavo anonimiziranih, sintetičnih ali drugih neosebni podatkov;
- (c) obstajajo učinkoviti mehanizmi za spremljanje, s katerimi se ugotovi, ali se med eksperimentiranjem v peskovniku lahko pojavijo velika tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, kot je navedeno v členu 35 Uredbe (EU) 2016/679 in členu 39 Uredbe (EU) 2018/1725, ter mehanizmi za odzivanje, s katerimi se ta tveganja nemudoma zmanjšajo in se po potrebi ustavi obdelava;
- (d) vsi osebni podatki, ki se obdelujejo v okviru peskovnika, so v funkcionalno ločenem, izoliranem in zaščitenem okolju za obdelavo podatkov pod nadzorom potencialnih ponudnikov, dostop do teh podatkov pa imajo le pooblašcene osebe;
- (e) ponudniki lahko prvotno zbrane podatke delijo naprej le v skladu s pravom Unije o varstvu podatkov; osebni podatkov ustvarjenih v peskovniku, ni mogoče deliti zunaj peskovnika;

- (f) nobena obdelava osebnih podatkov v okviru peskovnika ne sme biti podlaga za sprejetje ukrepov ali odločitev, ki bi vplivali na posameznike, na katere se nanašajo osebni podatki, niti ne sme vplivati na uveljavljanje njihovih pravic, določenih v pravu Unije o varstvu osebnih podatkov;
- (g) vsi osebni podatki, obdelani v okviru peskovnika, so zaščiteni z ustreznimi tehničnimi in organizacijskimi ukrepi in se izbrišejo, ko se sodelovanje v peskovniku konča ali ko se izteče obdobje hrambe osebnih podatkov;
- (h) dnevniki obdelave osebnih podatkov v okviru peskovnika se hranijo ves čas trajanja sodelovanja v peskovniku, razen če je v pravu Unije ali nacionalnem pravu določeno drugače;
- (i) celovit in podroben opis postopka in logike, na katerih temeljijo učenje, testiranje in validacija sistema UI, se skupaj z rezultati testiranja hrani kot del tehnične dokumentacije iz Priloge IV;
- (j) kratek povzetek projekta UI, razvitega v peskovniku, njegovi cilji in pričakovani rezultati so objavljeni na spletišču pristojnih organov; ta obveznost ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov mejne kontrole in organov, pristojnih za priseljevanje, ali azilnih organov.

2. Za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, pod nadzorom in odgovornostjo organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj obdelava osebnih podatkov v regulativnih peskovnikih za UI temelji na posebnem pravu Unije ali nacionalnem pravu in zanjo veljajo enaki kumulativni pogoji, kot so navedeni v odstavku 1.
3. Odstavek 1 ne posega v pravo Unije ali nacionalno pravo, ki izključuje obdelavo osebnih podatkov za druge namene, kot so izrecno navedeni v tem pravu, pa tudi ne v pravo Unije ali nacionalno pravo, ki določa podlago za obdelavo osebnih podatkov, potrebno za namene razvoja, testiranja ali učenja inovativnih sistemov UI, ali katero koli drugo pravno podlago, skladno s pravom Unije o varstvu osebnih podatkov.

Člen 60

Testiranje visokotveganih sistemov UI v realnih razmerah zunaj regulativnih peskovnikov za UI

1. Testiranje visokotveganih sistemov UI v realnih razmerah zunaj regulativnih peskovnikov za UI lahko izvajajo ponudniki ali potencialni ponudniki visokotveganih sistemov UI s seznama v Prilogi III v skladu s tem členom in načrtom testiranja v realnih razmerah iz tega člena, brez poseganja v prepovedi na podlagi člena 5.

Komisija z izvedbenimi akti določi podrobne elemente načrta testiranja v realnih razmerah. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

Ta odstavek ne posega v pravo Unije ali nacionalno pravo za testiranje visokotveganih sistemov UI, povezanih s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, v realnih razmerah.

2. Ponudniki ali potencialni ponudniki lahko testiranje visokotveganih sistemov UI iz Priloge III v realnih razmerah izvedejo kadar koli, preden dajo sistem UI na trg ali v uporabo, bodisi sami bodisi v partnerstvu z enim ali več uvajalci ali potencialnimi uvajalci.
3. Testiranje visokotveganih sistemov UI v realnih razmerah na podlagi tega člena ne posega v nobeno etično presojo, ki se zahteva v skladu s pravom Unije ali nacionalnim pravom.
4. Ponudniki ali potencialni ponudniki lahko testiranje v realnih razmerah izvajajo le, kadar so izpolnjeni vsi naslednji pogoji:
 - (a) ponudnik ali potencialni ponudnik je pripravil načrt testiranja v realnih razmerah in ga predložil organu za nadzor trga v državi članici, v kateri se bo testiranje v realnih razmerah izvajalo;
 - (b) organ za nadzor trga v državi članici, v kateri se testiranje v realnih razmerah izvaja, je odobril testiranje v realnih razmerah in načrt testiranja v realnih razmerah; kadar organ za nadzor trga ne odgovori v 30 dneh, se šteje, da sta testiranje v realnih razmerah in načrt testiranja v realnih razmerah odobrena; kadar nacionalno pravo ne določa tihe odobritve, je za testiranje v realnih razmerah še naprej potrebno dovoljenje;

- (c) ponudnik ali potencialni ponudnik, z izjemo ponudnikov ali potencialnih ponudnikov visokotveganih sistemov UI iz Priloge III, točke 1, 6 in 7, na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja nadzora meja ter visokotveganih sistemov UI iz Priloge III, točka 2, je registriral testiranje v realnih razmerah v skladu s členom 71(4) z vseevropsko enotno identifikacijsko številko in informacijami, določenimi v Prilogi IX; ponudnik ali potencialni ponudnik visokotveganih sistemov UI iz točk 1, 6 in 7 Priloge III je na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, migracij, azila in upravljanja mejnega nadzora registriral testiranje v realnih razmerah v varnem nejavnem delu podatkovne zbirke EU skladno s členom 49(4), točka (d), z vseevropsko enotno identifikacijsko številko in informacijami, določenimi v njej; ponudnik ali potencialni ponudnik visokotveganih sistemov UI iz točke 2 Priloge III je registriral testiranje v realnih razmerah v skladu s členom 49(5);
- (d) ponudnik ali potencialni ponudnik, ki izvaja testiranje v realnih razmerah, ima sedež v Uniji ali je imenoval pravnega zastopnika, ki ima sedež v Uniji;
- (e) podatki, zbrani in obdelani za namen testiranja v realnih razmerah, se v tretje države prenesejo le, če se izvajajo ustrezni in veljavni zaščitni ukrepi na podlagi prava Unije;

- (f) testiranje v realnih razmerah ne traja dlje, kot je potrebno, da se dosežejo zadani cilji, v nobenem primeru pa ne presega šestmesečnega obdobja, ki se lahko podaljša za dodatnih šest mesecev, če ponudnik ali potencialni ponudnik o tem predhodno uradno obvesti organ za nadzor trga in uradnemu obvestilu doda obrazložitev potrebe po takem podaljšanju;
- (g) udeleženci testiranja v realnih razmerah, ki so osebe, ki pripadajo ranljivim skupinam zaradi svoje starosti ali invalidnosti, so ustrezno zaščiteni;
- (h) kadar ponudnik ali potencialni ponudnik testiranje v realnih razmerah organizira v sodelovanju z enim ali več uvajalci ali potencialnimi uvajalci, so bili slednji obveščeni o vseh vidikih testiranja, ki so pomembni za njihovo odločitev za sodelovanje, in so prejeli ustrezna navodila za uporabo sistema UI iz člena 13; ponudnik ali potencialni ponudnik in uvajalec ali potencialni uvajalec sklenejo sporazum, ki določa njihove vloge in odgovornosti, da se zagotovi skladnost z določbami za testiranje v realnih razmerah na podlagi te uredbe ter na podlagi drugega veljavnega prava Unije in nacionalnega prava;
- (i) udeleženci testiranja v realnih razmerah so dali informirano privolitev v skladu s členom 61, v primeru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ko bi pridobitev informirane privolitve preprečila testiranje sistema UI, pa samo testiranje in rezultati testiranja v realnih razmerah ne smejo negativno vplivati na udeležence, njihovi osebni podatki pa se po koncu testiranja izbrišejo;

- (j) testiranje v realnih razmerah učinkovito nadzorujejo ponudnik ali potencialni ponudnik, pa tudi uvajalci ali potencialni uvajalci, z osebami, ki so ustrezno kvalificirane na zadevnem področju in imajo potrebne zmogljivosti, usposobljenost in pooblastila za opravljanje svojih nalog;
- (k) napovedi, priporočila ali odločitve sistema UI je mogoče učinkovito izničiti in zanemariti.

- 5. Vsi udeleženci testiranja v realnih razmerah ali njihov zakonito imenovani zastopnik, kot je primerno, se lahko brez kakršne koli škode in brez obrazložitve kadar koli umaknejo iz testiranja, tako, da prekličejo svojo informirano privolitev, in lahko zahtevajo, da se njihovi osebni podatki nemudoma in stalno izbrišejo. Preklic informirane privolitve ne vpliva na že izvedene dejavnosti.
- 6. Države članice v skladu s členom 75 na svoje organe za nadzor trga prenesejo pooblastila, na podlagi katerih od ponudnikov in potencialnih ponudnikov zahtevajo predložitev informacij, izvajajo nenapovedane inšpekcijske preglede na daljavo ali na kraju samem ter preverjajo opravljanje testiranja v realnih razmerah in z njimi povezane visoko tvegane sisteme UI. Organi za nadzor trga ta pooblastila uporabljajo za zagotovitev varnega poteka testiranja v realnih razmerah.

7. Vsak resen incident, ugotovljen med testiranjem v realnih razmerah, se sporoči nacionalnemu organu za nadzor trga v skladu s členom 73. Ponudnik ali potencialni ponudnik sprejme takojšnje ukrepe za zmanjšanje tveganj ali, če to ni mogoče, testiranje v realnih razmerah začasno ustavi, dokler ne pride do tovrstnega zmanjšanja, v nasprotnem primeru pa ga dokončno ustavi. Po taki dokončni ustavitvi testiranja v realnih razmerah vzpostavi postopek za takojšnji odpoklic sistema UI.
8. Ponudniki ali potencialni ponudniki obvestijo nacionalni organ za nadzor trga v državi članici, v kateri se testiranje v realnih razmerah izvaja, o začasni ali dokončni ustavitvi testiranja v realnih razmerah in o končnih rezultatih.
9. Ponudnik ali potencialni ponudnik je na podlagi veljavnega prava Unije in nacionalnega prava o odgovornosti odgovoren za vsakršno škodo, povzročeno med njegovim testiranjem v realnih razmerah.

Člen 61

Informirana privolitev za sodelovanje pri testiranju v realnih razmerah zunaj regulativnih peskovnikov za UI

1. Za namen testiranja v realnih razmerah na podlagi člena 60 udeleženci testiranja dajo prostovoljno informirano privolitev, preden začnejo sodelovati pri takem testiranju in po tem, ko so bili z jedrnatimi, jasnimi, ustreznimi in razumljivimi informacijami ustrezno obveščeni o:
 - (a) naravi in ciljih testiranja v realnih razmerah ter morebitnih nevšečnostih, ki so lahko povezane z njihovim sodelovanjem;
 - (b) pogojih, pod katerimi se bo testiranje v realnih razmerah izvajalo, vključno s pričakovanim trajanjem sodelovanja udeležencev;
 - (c) svojih pravicah in zagotovilih v zvezi s sodelovanjem, zlasti o pravici, da zavrnejo sodelovanje in se lahko brez kakršne koli škode in brez obrazložitve kadar koli umaknejo iz testiranja v realnih razmerah;
 - (d) tem, kako se vloži zahteva za to, da se napovedi, priporočila ali odločitve sistema UI izničijo ali zanemarijo;
 - (e) vseevropski enotni identifikacijski številki testiranja v realnih razmerah v skladu s členom 60(4), točka (c), in kontaktnih podatkih ponudnika ali njegovega pravnega zastopnika, od katerega je mogoče pridobiti dodatne informacije.

2. Informirana privolitev se datira in dokumentira, udeleženci testiranja ali njihov zakoniti zastopnik pa prejmejo kopijo.

Člen 62

Ukrepi za ponudnike in uvajalce, zlasti MSP, vključno z zagonskimi podjetji

1. Države članice sprejmejo naslednje ukrepe:
 - (a) MSP, vključno z zagonskimi podjetji, ki imajo statutarni sedež ali podružnico v Uniji, zagotovijo prednostni dostop do regulativnih peskovnikov za UI, če izpolnjujejo pogoje za upravičenost in merila za izbor; prednostni dostop drugim MSP, vključno z zagonskimi podjetji, razen tistih iz tega odstavka, ne preprečuje dostopa do regulativnega peskovnika za UI, če izpolnjujejo tudi pogoje za upravičenost in merila za izbor;
 - (b) organizirajo posebne dejavnosti ozaveščanja in usposabljanja o uporabi te uredbe, prilagojene potrebam MSP, vključno z zagonskimi podjetji, uvajalcev in, če je to primerno, lokalnih javnih organov;
 - (c) uporabijo obstoječe in, kadar je primerno, vzpostavijo nove posebne kanale za komunikacijo z MSP, vključno z zagonskimi podjetji, uvajalci, drugimi inovatorji in, če je to primerno, lokalnimi javnimi organi, da jim svetujejo in odgovarjajo na vprašanja o izvajanju te uredbe, tudi kar zadeva sodelovanje v regulativnih peskovnikih za UI;

- (d) olajšujejo sodelovanje MSP in drugih ustreznih deležnikov v postopku razvoja standardizacije.
2. Pri določanju pristojbin za ugotavljanje skladnosti na podlagi člena 43 se upoštevajo posebni interesi in potrebe ponudnikov, ki so MSP, vključno z zagonskimi podjetji, pri čemer se te pristojbine znižajo sorazmerno z njihovo velikostjo, velikostjo trga in drugimi ustreznimi kazalniki.
3. Urad za UI sprejme naslednje ukrepe:
- (a) zagotovi standardizirane predloge za področja, ki jih zajema ta uredba, kot jih določi Odbor v svoji zahtevi;
 - (b) razvija in vzdržuje enotno informacijsko platformo, na kateri so vsem operaterjem po vsej Uniji na voljo informacije v zvezi s to uredbo, ki so enostavne za uporabo;
 - (c) organizira ustrezne komunikacijske kampanje za ozaveščanje o obveznostih, ki izhajajo iz te uredbe;
 - (d) ocenjuje in spodbuja zbliževanja najboljših praks v postopkih javnega naročanja v zvezi s sistemi UI.

Člen 63

Odstopanja za določene operaterje

1. Mikropodjetja v smislu Priporočila 2003/361/ES lahko nekatere elemente sistema vodenja kakovosti iz člena 17 te uredbe izpolnjujejo na poenostavljen način, če nimajo partnerskih podjetij ali povezanih podjetij v smislu navedenega priporočila. V ta namen Komisija pripravi smernice o elementih sistema vodenja kakovosti, ki se lahko upoštevajo na poenostavljen način ob upoštevanju potreb mikropodjetij, ne da bi to vplivalo na raven zaščite ali potrebo po skladnosti z zahtevami v zvezi z visokotveganimi sistemi UI.
2. Odstavek 1 tega člena se ne razlaga tako, da so ti operaterji oproščeni izpolnjevanja katerih koli drugih zahtev ali obveznosti iz te uredbe, tudi tistih ne iz členov 9, 10, 11, 12, 13, 14, 15, 72 in 73.

Poglavje VII

Upravljanje

ODDELEK 1

UPRAVLJANJE NA RAVNI UNIJE

Člen 64

Urad za UI

1. Komisija prek Urada za UI razvija strokovno znanje in zmogljivosti Unije na področju UI.
2. Države članice olajšujejo naloge, zaupane Uradu za UI, kot je razvidno iz te uredbe.

Člen 65

Ustanovitev in struktura Evropskega odbora za umetno inteligenco

1. Ustanovi se Evropski odbor za umetno inteligenco (v nadaljnjem besedilu: Odbor).

2. Odbor sestavlja po en predstavnik vsake države članice. Evropski nadzornik za varstvo podatkov sodeluje kot opazovalec. Sestankov Odbora se udeležuje tudi Urad za UI, pri glasovanju pa ne sodeluje. Odbor se lahko vsakič posebej odloči, da na sestanek povabi druge organe, telesa ali strokovnjake iz Unije in držav članic, kadar so obravnavana vprašanja zanje pomembna.
3. Države članice imenujejo svojega predstavnika za obdobje treh let z možnostjo enkratnega podaljšanja.
4. Države članice zagotovijo, da njihovi predstavniki v Odboru:
 - (a) imajo v svoji državi članici ustrezne pristojnosti in pooblastila, da dejavno prispevajo k izpolnjevanju nalog Odbora iz člena 66;
 - (b) so določeni kot enotna kontaktna točka v odnosu do Odbora in, kadar je primerno, ob upoštevanju potreb držav članic kot enotna kontaktna točka za deležnike;
 - (c) so pooblaščen za spodbujanje doslednosti in usklajevanja med pristojnimi nacionalnimi organi v svoji državi članici glede izvajanja te uredbe, vključno z zbiranjem ustreznih podatkov in informacij za namene opravljanja njihovih nalog v Odboru.
5. Imenovani predstavniki držav članic z dvotretjinsko večino sprejmejo poslovnik Odbora. V poslovniku se določijo zlasti potek izbirnega postopka, trajanje mandata predsednika in specifikacije njegovih nalog, podrobnosti glede glasovanja ter organizacija dejavnosti Odbora in dejavnosti njegovih podskupin.

6. Odbor ustanovi dve stalni podskupini, da bi zagotavljali platformo za sodelovanje in izmenjavo med organi za nadzor trga ter uradno obveščali organe o vprašanjih, povezanih z nadzorom trga oziroma priglasienimi organi.

Stalna podskupina za nadzor trga bi morala delovati kot skupina za upravno koordinacijo (ADCO) za to uredbo v smislu člana 30 Uredbe (EU) 2019/1020.

Odbor lahko ustanovi druge bodisi stalne ali začasne podskupine za preučitev posebnih vprašanj. Po potrebi so lahko predstavniki svetovalnega foruma iz člana 67 povabljeni k sodelovanju v takih podskupinah ali na posebne seitanke teh podskupin kot opazovalci.

7. Odbor je organiziran in se upravlja tako, da zagotavlja objektivnost in nepristranskost svojih dejavnosti.
8. Odboru predseduje eden od predstavnikov držav članic. Urad za UI je sekretariat Odbora, na zahtevo predsednika sklicuje seitanke in pripravi njihov dnevni red v skladu z nalogami Odbora na podlagi te uredbe in njegovega poslovnika.

Člen 66
Naloge Odbora

Odbor svetuje in pomaga Komisiji in državam članicam, da se olajša dosledna in učinkovita uporaba te uredbe. V ta namen lahko Odbor zlasti:

- (a) prispeva k usklajevanju med pristojnimi nacionalnimi organi, odgovornimi za uporabo te uredbe, ter v sodelovanju z zadevnimi organi za nadzor trga in v dogovoru z njimi podpira skupne dejavnosti organov za nadzor trga iz člena 74(11);
- (b) zbira in izmenjuje tehnično in regulativno strokovno znanje in najboljše prakse med državami članicami;
- (c) svetuje o izvajanju te uredbe, zlasti v zvezi z izvrševanjem pravil o modelih UI za splošne namene;
- (d) prispeva k harmonizaciji upravnih praks v državah članicah, tudi v zvezi z odstopanjem od postopkov ugotavljanja skladnosti iz člena 46, delovanjem regulativnih peskovnikov za UI ter testiranjem v realnih razmerah iz členov 57, 59 in 60;

- (e) na zahtevo Komisije ali na lastno pobudo izda priporočila in pisna mnenja o vseh pomembnih zadevah v zvezi z izvajanjem te uredbe ter njeno dosledno in učinkovito uporabo, tudi:
- (i) o razvoju in uporabi kodeksov ravnanja in kodeksov prakse na podlagi te uredbe ter smernic Komisije;
 - (ii) o oceni in pregledu te uredbe na podlagi člena 112, tudi kar zadeva poročila o resnih incidentih iz člena 73 in delovanje podatkovne zbirke EU iz člena 71, o pripravi delegiranih ali izvedbenih aktov ter morebitnih uskladitvah te uredbe s pravnimi akti iz Priloge I;
 - (iii) o tehničnih specifikacijah ali obstoječih standardih v zvezi z zahtevami iz poglavja III, oddelek 2,
 - (iv) o uporabi harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41;
 - (v) o trendih, kot so svetovna konkurenčnost Evrope na področju UI, uvajanje UI v Uniji ter razvoj digitalnih spretnosti;
 - (vi) o trendih v zvezi z razvijajočo se tipologijo verig vrednosti UI, zlasti glede iz tega izhajajočih posledic v smislu odgovornosti;

- (vii) o morebitni potrebi po spremembi Priloge III v skladu s členom 7 in o morebitni potrebi po morebitni reviziji člena 5 na podlagi člena 112, ob upoštevanju ustreznih razpoložljivih dokazov in najnovejšega tehnološkega razvoja;
- (f) podpira Komisijo pri spodbujanju pismenosti na področju UI ter ozaveščanja in razumevanja javnosti o prednostih, tveganjih, zaščitnih ukrepih ter pravicah in obveznostih, povezanih z uporabo sistemov UI;
- (g) spodbuja oblikovanje skupnih meril in skupnega razumevanja ustreznih konceptov iz te uredbe med udeleženci na trgu in pristojnimi organi, tudi s prispevanjem k razvoju meril uspešnosti;
- (h) sodeluje, če je to primerno, z drugimi institucijami, organi, uradi in agencijami Unije, pa tudi z ustreznimi strokovnimi skupinami in mrežami Unije, zlasti na področju varnosti proizvodov, kibernetске varnosti, konkurence, digitalnih in medijskih storitev, finančnih storitev, varstva potrošnikov ter varstva podatkov in temeljnih pravic;
- (i) prispeva k učinkovitemu sodelovanju s pristojnimi organi tretjih držav in mednarodnimi organizacijami;
- (j) pomaga pristojnim nacionalnim organom in Komisiji pri razvoju organizacijskega in tehničnega strokovnega znanja, potrebnega za izvajanje te uredbe, vključno s prispevanjem k oceni potreb po usposabljanju osebja držav članic, ki sodeluje pri izvajanju te uredbe;

- (k) pomaga Uradu za UI pri podpiranju pristojnih nacionalnih organov pri vzpostavitvi in razvoju regulativnih peskovnikov za UI ter olajšuje sodelovanje in izmenjavo informacij med regulativnimi peskovniki za UI;
- (l) prispeva k pripravi smernic in zagotavlja ustrezno svetovanje v zvezi z njim;
- (m) svetuje Komisiji v zvezi z mednarodnimi zadevami na področju UI;
- (n) Komisiji daje mnenja o kvalificiranih opozorilih v zvezi z modeli UI za splošne namene;
- (o) prejema mnenja držav članic o kvalificiranih opozorilih v zvezi z modeli UI za splošne namene ter o nacionalnih izkušnjah in praksah v zvezi s spremljanjem in izvrševanjem sistemov UI, zlasti sistemov, v katere so vgrajeni modeli UI za splošne namene.

Člen 67

Svetovalni forum

1. Ustanovi se svetovalni forum, ki zagotavlja tehnično strokovno znanje in svetuje Odboru in Komisiji ter prispeva k njunim nalogam iz te uredbe.
2. Članstvo svetovalnega foruma je sestavljeno iz uravnoteženega izbora deležnikov, vključno z industrijo, zagonskimi podjetji, MSP, civilno družbo in akademskimi krogi. Članstvo v svetovalnem forumu je uravnoteženo z vidika komercialnih in nekomercialnih interesov, v kategoriji poslovnih interesov pa z vidika MSP in drugih podjetij.

3. Komisija člane svetovalnega foruma imenuje med deležniki s priznanim strokovnim znanjem na področju UI v skladu z merili iz odstavka 2.
4. Mandat članov svetovalnega foruma traja dve leti in se lahko podaljša še za največ štiri leta.
5. Stalni člani svetovalnega foruma so Agencija Evropske unije za temeljne pravice, ENISA, Evropski odbor za standardizacijo (CEN), Evropski odbor za elektrotehniško standardizacijo (CENELEC) in Evropski inštitut za telekomunikacijske standarde (ETSI).
6. Svetovalni forum sestavi svoj poslovnik. Med svojimi člani izvoli dva sopredsednika v skladu z merili iz odstavka 2. Mandat sopredsednikov traja dve leti z možnostjo enkratnega podaljšanja.
7. Svetovalni forum se sestane najmanj dvakrat na leto. Na svoje sestanke lahko povabi strokovnjake in druge deležnike.
8. Svetovalni forum lahko na zahtevo Odbora ali Komisije pripravi mnenja, priporočila in pisne prispevke.
9. Svetovalni forum lahko po potrebi ustanovi stalne ali začasne podskupine za preučitev posebnih vprašanj, povezanih s cilji te uredbe.
10. Svetovalni forum pripravi letno poročilo o svojih dejavnostih. To poročilo se objavi.

Člen 68

Znanstveni odbor neodvisnih strokovnjakov

1. Komisija z izvedbenim aktom sprejme določbe o ustanovitvi znanstvenega odbora neodvisnih strokovnjakov (v nadaljnjem besedilu: znanstveni odbor), ki bo podpiral dejavnosti izvrševanja iz te uredbe. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).
2. Znanstveni odbor sestavljajo strokovnjaki, ki jih Komisija izbere na podlagi najnovejšega znanstvenega ali tehničnega strokovnega znanja na področju UI, potrebnega za naloge iz odstavka 3, in so sposobni dokazati, da izpolnjujejo vse naslednje pogoje:
 - (a) imajo posebno strokovno znanje in kompetence ter znanstveno ali tehnično strokovno znanje na področju UI;
 - (b) neodvisnost od katerega koli ponudnika sistemov UI ali modelov UI za splošne namene;
 - (c) sposobnost skrbnega, natančnega in objektivnega izvajanja dejavnosti.

Komisija v posvetovanju z Odborom in v skladu z zahtevanimi potrebami določi število strokovnjakov v znanstvenem odboru ter zagotovi pravično zastopanost spolov in geografsko zastopanost.

3. Znanstveni odbor svetuje Uradu za UI in mu zagotavlja podporo, zlasti v zvezi z naslednjimi nalogami:
- (a) podpiranje izvajanja in izvrševanja te uredbe v zvezi z modeli UI in sistemi za splošne namene, zlasti z:
 - (i) opozarjanjem Urada za UI na morebitna sistemska tveganja, ki jih lahko na ravni Unije povzročajo modeli UI za splošne namene, v skladu s členom 90;
 - (ii) prispevanjem k razvoju orodij in metodologij za ocenjevanje zmogljivosti modelov UI in sistemov za splošne namene, vključno z merili uspešnosti;
 - (iii) svetovanjem o razvrstitvi modelov UI za splošne namene s sistemskim tveganjem;
 - (iv) svetovanjem o razvrstitvi različnih modelov UI in sistemov za splošne namene;
 - (v) prispevanjem k razvoju orodij in predlog;
 - (b) podpiranje dela organov za nadzor trga na njihovo zahtevo;
 - (c) podpiranje čezmejnih dejavnosti nadzora trga iz člena 74(11), brez poseganja v pooblastila organov za nadzor trga;

(d) podpiranje Urada za UI pri opravljanju njegovih nalog v okviru zaščitnega postopka Unije na podlagi člena 81.

4. Strokovnjaki znanstvenega odbora svoje naloge opravljajo nepristransko in objektivno ter zagotavljajo zaupnost informacij in podatkov, pridobljenih pri izvajanju njihovih nalog in dejavnosti. Pri opravljanju svojih nalog iz odstavka 3 ne smejo zahtevati ali sprejemati navodil od nikogar. Vsak strokovnjak predloži izjavo o interesih, ki se tudi objavi. Urad za UI vzpostavi sisteme in postopke za aktivno obvladovanje in preprečevanje morebitnih nasprotij interesov.
5. Izvedbeni akt iz odstavka 1 vključuje določbe o pogojih, postopkih in podrobnostih, v skladu s katerimi znanstveni odbor in njegovi člani izdajajo opozorila in zapošajo Urad za UI za pomoč pri opravljanju svojih nalog.

Člen 69

Dostop držav članic do nabora strokovnjakov

1. Države članice lahko strokovnjake znanstvenega sveta zaprosijo, da jim pomagajo pri dejavnostih izvrševanja iz te uredbe.

2. Od držav članic se lahko zahteva, da plačajo pristojbine za svetovanje in podporo strokovnjakov. Struktura in višina pristojbin ter višina in struktura povračljivih stroškov se določi v izvedbenem aktu iz člena 68(1), pri čemer se upoštevajo cilji ustreznega izvajanja te uredbe, stroškovna učinkovitost in potreba, da se vsem državam članicam zagotovi učinkovit dostop do strokovnjakov.
3. Komisija državam članicam po potrebi omogoči pravočasen dostop do strokovnjakov in zagotovi, da je kombinacija podpornih dejavnosti, ki jih izvajajo podporne strukture Unije za testiranje UI na podlagi člena 84, in strokovnjakov na podlagi tega člena učinkovito organizirana in zagotavlja največjo možno dodano vrednost.

ODDELEK 2

PRISTOJNI NACIONALNI ORGANI

Člen 70

Imenovanje pristojnih nacionalnih organov in enotne kontaktne točke

1. Za namene te uredbe vsaka država članica kot pristojne nacionalne organe ustanovi ali imenuje vsaj en priglasitveni organ in vsaj en organ za nadzor trga. Ti pristojni nacionalni organi svoja pooblastila izvajajo neodvisno, nepristransko in brez predsodkov, da bi zaščitili objektivnost svojih dejavnosti in nalog ter zagotovili uporabo in izvajanje te uredbe. Člani teh organov se vzdržijo vseh dejanj, ki niso združljiva z njihovimi dolžnostmi. Če se ta načela spoštujejo, lahko take dejavnosti in naloge izvaja eden ali več imenovanih organov v skladu z organizacijskimi potrebami države članice.
2. Države članice Komisiji sporočijo identiteto priglasitvenih organov in organov za nadzor trga ter njihove naloge in vse naknadne spremembe v zvezi s tem. Države članice do ... [12 mesecev od datuma začetka veljavnosti te uredbe] prek elektronskih komunikacijskih sredstev objavijo informacije o tem, kako je mogoče stopiti v stik s pristojnimi organi in enotnimi kontaktnimi točkami. Države članice imenujejo organ za nadzor trga, ki deluje kot enotna kontaktna točka za to uredbo, in Komisijo uradno obvestijo o identiteti enotne kontaktne točke. Komisija seznam enotnih kontaktnih točk objavi.

3. Države članice zagotovijo, da imajo njihovi pristojni nacionalni organi na voljo ustrezne tehnične, finančne in človeške vire ter infrastrukturo za učinkovito izpolnjevanje svojih nalog na podlagi te uredbe. Pristojni nacionalni organi morajo imeti zlasti zadostno število stalno razpoložljivega osebja, katerega kompetence in strokovno znanje vključujejo poglobljeno razumevanje tehnologij UI, podatkov in računalniške obdelave podatkov, varstva osebnih podatkov, kibernetске varnosti, temeljnih pravic, zdravstvenih in varnostnih tveganj ter poznavanje obstoječih standardov in pravnih zahtev. Države članice vsako leto ocenijo in po potrebi posodobijo zahteve glede usposobljenosti in virov iz tega odstavka.
4. Pristojni nacionalni organi sprejmejo ustrezne ukrepe, da se zagotovi ustrezna raven kibernetске varnosti.
5. Pristojni nacionalni organi pri opravljanju svojih nalog delujejo v skladu z obveznostmi glede zaupnosti iz člena 78.
6. Države članice do ... [eno leto od datuma začetka veljavnosti te uredbe] in nato vsaki dve leti poročajo Komisiji o stanju finančnih in človeških virov, ki so na voljo pristojnim nacionalnim organom, z oceno njihove ustreznosti. Komisija navedene informacije posreduje Odboru v razpravo in morebitna priporočila.
7. Komisija olajšuje izmenjavo izkušenj med pristojnimi nacionalnimi organi.

8. Pristojni nacionalni organi lahko zagotovijo smernice in nasvete o izvajanju te uredbe, zlasti za MSP, vključno z zagonskimi podjetji, pri čemer po potrebi upoštevajo smernice in nasvete Odbora in Komisije. Kadar nameravajo pristojni nacionalni organi zagotoviti smernice in nasvete v zvezi s sistemom UI na področjih, ki jih zajema drugo pravo Unije, se, če je to primerno, posvetujejo s pristojnimi nacionalnimi organi, ki delujejo na podlagi navedenega prava Unije.
9. Kadar institucije, organi, uradi in agencije Unije spadajo na področje uporabe te uredbe, Evropski nadzornik za varstvo podatkov deluje kot pristojni organ za njihov nadzor.

Poglavje VIII

Podatkovna zbirka EU za visokotvegane sisteme UI

Člen 71

Podatkovna zbirka EU za visokotvegane sisteme UI s seznama v Prilogi III

1. Komisija v sodelovanju z državami članicami vzpostavi in vzdržuje podatkovno zbirko EU, ki vsebuje informacije iz odstavkov 2 in 3 tega člena o visokotveganih sistemih UI iz člena 6(2), registriranih v skladu s členoma 49 in 60, ter sisteme UI, ki se ne štejejo za visokotvegane na podlagi člena 6(3) in ki so registrirani v skladu s členom 6(4) in členom 49. Komisija se pri določanju funkcionalnih specifikacij take podatkovne zbirke posvetuje z ustreznimi strokovnjaki, pri posodabljanju funkcionalnih specifikacij take podatkovne zbirke pa z Odborom.

2. Podatke iz Priloge VIII, oddelka A in B, v podatkovno zbirko EU vnese ponudnik ali po potrebi pooblaščen zastopnik.
3. Podatke iz Priloge VIII, oddelek C, v podatkovno zbirko EU vnese uvajalec, ki je javni organ, agencija ali telo ali deluje v njegovem imenu, v skladu s členom 49(3) in (4).
4. Z izjemo oddelka iz člena 49(4) in člena 60(4), točka (c), so informacije v podatkovni zbirki EU, registrirane v skladu s členom 49, dostopne in na voljo javnosti na uporabniku prijazen način. Po informacijah bi se moralo dati enostavno iskati in morale bi biti strojno berljive. Informacije, registrirane v skladu s členom 60, so dostopne samo organom za nadzor trga in Komisiji, razen če je potencialni ponudnik ali ponudnik dal soglasje, da so te informacije dostopne tudi javnosti.
5. Podatkovna zbirka EU vsebuje osebne podatke le, kolikor je to potrebno za zbiranje in obdelavo informacij v skladu s to uredbo. Te informacije vključujejo imena in kontaktne podatke fizičnih oseb, ki so odgovorne za registracijo sistema in imajo pravno pooblastilo za zastopanje ponudnika ali uvajalca, kakor je ustrezno.
6. Komisija je upravljavec podatkovne zbirke EU. Ponudnikom, potencialnim ponudnikom in uvajalcem zagotavlja ustrezno tehnično in upravno podporo. Podatkovna zbirka EU mora biti skladna z veljavnimi zahtevami glede dostopnosti.

Poglavje IX

Spremljanje po dajanju na trg, izmenjava informacij in nadzor trga

ODDELEK 1

SPREMLJANJE PO DAJANJU NA TRG

Člen 72

Spremljanje po dajanju na trg s strani ponudnikov in načrt spremljanja po dajanju na trg za visokotvegane sisteme UI

1. Ponudniki vzpostavijo in dokumentirajo sistem spremljanja po dajanju na trg na način, ki je sorazmeren z naravo tehnologij UI in tveganji visokotvegane sistema UI.
2. Sistem spremljanja po dajanju na trg aktivno in sistematično zbira, dokumentira in analizira ustrezne podatke o učinkovitosti visokotveganih sistemov UI skozi celotno življenjsko dobo, ki jih lahko zagotovijo uvajalci ali ki se lahko zberejo prek drugih virov ter ki ponudniku omogočajo, da oceni, ali sistemi UI stalno izpolnjujejo zahteve iz poglavja III, oddelek 2. Kadar je ustrezno, spremljanje po dajanju na trg vključuje analizo interakcije z drugimi sistemi UI. Ta obveznost ne zajema občutljivih operativnih podatkov uvajalcev, ki so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj.

3. Sistem spremljanja po dajanju na trg temelji na načrtu spremljanja po dajanju na trg. Načrt spremljanja po dajanju na trg je del tehnične dokumentacije iz Priloge IV. Komisija sprejme izvedbeni akt s podrobnimi določbami o predlogi za načrt spremljanja po dajanju na trg in s seznamom elementov, ki jih je treba do ... [18 mesecev od začetka veljavnosti te uredbe] vključiti v načrt. Ta izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 98(2).
4. Za visokotvegane sisteme UI, zajete v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A – kadar sta sistem in načrt spremljanja po dajanju na trg že vzpostavljena na podlagi navedene zakonodaje in da se zagotovi skladnost, prepreči podvajanje in čim bolj zmanjšajo dodatna bremena – imajo ponudniki možnost, da v sisteme in načrte, ki že obstajajo na podlagi navedene zakonodaje, po potrebi vključijo potrebne elemente, opisane v odstavkih 1, 2 in 3, pri čemer uporabijo predlogo iz odstavka 3, če se s tem doseže enakovredna raven zaščite.

Prvi pododstavek tega odstavka se uporablja tudi za visokotvegane sisteme UI iz Priloge III, točka 5, ki jih dajo na trg ali v uporabo finančne institucije, za katere veljajo zahteve na podlagi prava Unije o finančnih storitvah v zvezi z njihovim notranjim upravljanjem, ureditvami ali postopki.

ODDELEK 2

IZMENJAVA INFORMACIJ O RESNIH INCIDENTIH

Člen 73

Poročanje o resnih incidentih

1. Ponudniki visokotveganih sistemov UI, ki so dani na trg Unije, organom za nadzor trga držav članic, v katerih je prišlo do navedenega incidenta, poročajo o vsakem resnem incidentu.
2. Poročilo iz odstavka 1 se sestavi takoj, ko ponudnik ugotovi obstoj vzročne zveze med sistemom UI in resnim incidentom ali razumno verjetnost take zveze, v vsakem primeru pa najpozneje 15 dni po tem, ko ponudnik ali, kadar je ustrezno, uvajalec izve za resen incident.

Pri roku za poročanje iz prvega pododstavka se upošteva resnost incidenta.

3. Ne glede na odstavek 2 tega člena se v primeru močno razširjene kršitve ali resnega incidenta, kakor je opredeljen v členu 3, točka 49(b), poročilo iz odstavka 1 predloži nemudoma, najpozneje pa dva dni po tem, ko ponudnik ali, kadar je ustrezno, uvajalec izve za ta incident.

4. Ne glede na odstavek 2 se v primeru smrti osebe poročilo predloži takoj, ko ponudnik ali uvajalec ugotovi ali posumi, da obstaja vzročna zveza med visokotveganim sistemom UI in resnim incidentom, vendar najpozneje 10 dni po datumu, ko ponudnik ali, kadar je ustrezno, uvajalec izve za resen incident.
5. Kadar je to potrebno zaradi pravočasnega poročanja, lahko ponudnik ali, kadar je ustrezno, uvajalec najprej predloži nepopolno začetno poročilo, nato pa predloži še popolnega.
6. Po poročanju o resnem incidentu na podlagi odstavka 1 ponudnik nemudoma izvede potrebne preiskave v zvezi z resnim incidentom in zadevnim sistemom UI. To vključuje oceno tveganja incidenta in popravne ukrepe.

Ponudnik med preiskavami iz prvega pododstavka sodeluje s pristojnimi organi in po potrebi z zadevnim priglasišenim organom ter brez predhodne obvestitve pristojnih organov ne izvede nobene raziskave, ki vključuje spremembo zadevnega sistema UI na način, ki bi lahko vplival na poznejšo oceno vzrokov za incident.

7. Zadevni organ za nadzor trga po prejemu uradnega obvestila o resnem incidentu iz člena 3, točka 49(c), obvesti nacionalne javne organe ali telesa iz člena 77(1). Komisija pripravi posebne smernice za lažje izpolnjevanje obveznosti iz odstavka 1 tega člena. Navedene smernice se izdajo do ... [12 mesecev od začetka veljavnosti te uredbe] in se redno ocenjujejo.

8. Organ za nadzor trga sprejme ustrezne ukrepe, kot je določeno v členu 19 Uredbe (EU) 2019/1020, v sedmih dneh od datuma prejema uradnega obvestila iz odstavka 1 tega člena in upošteva postopke uradnega obveščanja iz navedene uredbe.
9. Za visokotvegane sisteme UI iz Priloge III, ki jih dajejo na trg ali v uporabo ponudniki, za katere veljajo zakonodajni instrumenti Unije, v katerih so določene obveznosti glede poročanja, enakovredne tistim iz te uredbe, se uradno obveščanje o resnih incidentih zahteva le za incidente iz člena 3, točka 49(c).
10. Za visokotvegane sisteme UI, ki so varnostne komponente pripomočkov ali so sami pripomočki, zajeti v uredbah (EU) 2017/745 in (EU) 2017/746, je uradno obvestilo o resnih incidentih omejeno na tiste iz člena 3, točka 49(c), te uredbe in se pošlje pristojnemu nacionalnemu organu, ki ga v ta namen izberejo države članice, v katerih se je navedeni incident zgodil.
11. Pristojni nacionalni organi v skladu s členom 20 Uredbe (EU) 2019/1020 nemudoma uradno obvestijo Komisijo o vsakem resnem incidentu, ne glede na to, ali so v zvezi z njim ukrepali ali ne.

ODDELEK 3

IZVRŠEVANJE

Člen 74

Nadzor trga in nadzor sistemov UI na trgu Unije

1. Za sisteme UI, zajete s to uredbo, se uporablja Uredba (EU) 2019/1020. Za učinkovito izvrševanje te uredbe velja naslednje:
 - (a) vsako sklicevanje na gospodarski subjekt na podlagi Uredbe (EU) 2019/1020 se razume kot sklicevanje na vse operaterje, opredeljene v členu 2(1) te uredbe;
 - (b) vsako sklicevanje na proizvod na podlagi Uredbe (EU) 2019/1020 se razume kot sklicevanje na vse sisteme UI, ki spadajo na področje uporabe te uredbe.
2. Organi za nadzor trga v okviru svojih obveznosti poročanja na podlagi člena 34(4) Uredbe (EU) 2019/1020 Komisiji in ustreznim nacionalnim organom za konkurenco vsako leto poročajo o vseh informacijah, ugotovljenih med dejavnostmi nadzora trga, ki bi lahko bile zanimive za uporabo prava Unije o pravilih konkurence. Komisiji vsako leto poročajo tudi o primerih uporabe prepovedanih praks, do katerih je prišlo v zadevnem letu, in o sprejetih ukrepih.
3. Za visokotvegane sisteme UI, ki so povezani s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, je organ za nadzor trga za namene te uredbe organ, odgovoren za dejavnosti nadzora trga in imenovan v skladu z navedenimi pravnimi akti.

Z odstopanjem od prvega pododstavka in v ustreznih okoliščinah lahko države članice imenujejo drug ustrezen organ, ki deluje kot organ za nadzor trga, če zagotovijo usklajevanje z ustreznimi sektorskimi organi za nadzor trga, odgovornimi za izvrševanje harmonizacijske zakonodaje Unije iz Priloge I.

4. Postopki iz členov 79 do 83 te uredbe se ne uporabljajo za sisteme UI, ki so povezani s proizvodi, zajetimi v harmonizacijski zakonodaji Unije iz Priloge I, oddelek A, če so v takih pravnih aktih že določeni postopki, na podlagi katerih se zagotovi enakovredna raven zaščite in ki imajo isti cilj. V takih primerih se namesto tega uporabijo ustrezni sektorski postopki.
5. Brez poseganja v pooblastila organov za nadzor trga na podlagi člena 14 Uredbe (EU) 2019/1020 lahko organi za nadzor trga, da se zagotovi učinkovito izvrševanje te uredbe, pooblastila iz člena 14(4), točki (d) in (j), navedene uredbe po potrebi izvajajo na daljavo.
6. Za visokotvegane sisteme UI, ki jih dajo na trg ali v uporabo oziroma jih uporabljajo finančne institucije, ki jih ureja pravo Unije o finančnih storitvah, je organ za nadzor trga za namene te uredbe zadevni nacionalni organ, odgovoren za finančni nadzor navedenih institucij na podlagi navedene zakonodaje, če je dajanje sistema UI na trg ali v uporabo oziroma njegova uporaba neposredno povezana z zagotavljanjem navedenih finančnih storitev.

7. Z odstopanjem od odstavka 6 lahko država članica v ustreznih okoliščinah in pod pogojem, da je zagotovljeno usklajevanje, za organ za nadzor trga za namene te uredbe določi drug zadevni organ.

Nacionalni organi za nadzor trga, ki nadzorujejo regulirane kreditne institucije, ki jih ureja Direktiva 2013/36/EU, in sodelujejo v enotnem mehanizmu nadzora, vzpostavljenem z Uredbo (EU) št. 1024/2013, bi morali Evropski centralni banki brez odlašanja sporočiti vse informacije, ugotovljene v okviru svojih dejavnosti nadzora trga, ki bi lahko bile zanimive za naloge bonitetnega nadzora Evropske centralne banke, kot so določene v navedeni uredbi.

8. Za visokotvegane sisteme UI iz točke 1 Priloge III k tej uredbi, če se sistemi uporabljajo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, upravljanja meja ter pravosodja in demokracije, in za visokotvegane sisteme UI iz Priloge III, točke 6, 7 in 8, k tej uredbi države članice kot organe za nadzor trga za namene te uredbe imenujejo bodisi pristojne nadzorne organe za varstvo podatkov na podlagi Uredbe (EU) 2016/679 ali Direktive (EU) 2016/680 bodisi kateri koli drugi organ, ki je imenovan na podlagi enakih pogojev iz členov 41 do 44 Direktive (EU) 2016/680. Dejavnosti nadzora trga nikakor ne vplivajo na neodvisnost pravosodnih organov in tudi drugače ne posegajo v njihove dejavnosti, kadar delujejo v okviru svoje sodne pristojnosti.

9. Kadar institucije, organi, uradi in agencije Unije spadajo na področje uporabe te uredbe, Evropski nadzornik za varstvo podatkov deluje kot njihov organ za nadzor trga, razen v zvezi s Sodiščem Evropske unije, kadar to izvaja svojo sodno pristojnost.
10. Države članice olajšujejo usklajevanje med organi za nadzor trga, imenovanimi na podlagi te uredbe, in drugimi ustreznimi nacionalnimi organi ali telesi, ki nadzorujejo uporabo harmonizacijske zakonodaje Unije iz Priloge I ali drugega prava Unije, ki bi lahko bilo pomembno za visokotvegane sisteme UI iz Priloge III.
11. Organi za nadzor trga in Komisija lahko predlagajo skupne dejavnosti – vključno s skupnimi preiskavami, ki jih izvajajo organi za nadzor trga sami ali skupaj s Komisijo –, katerih cilj je spodbujanje skladnosti, odkrivanje neskladnosti, ozaveščanje ali zagotavljanje smernic v zvezi s to uredbo, kar zadeva posebne kategorije visokotveganih sistemov UI, za katere se ugotovi, da predstavljajo resno tveganje v dveh ali več državah članicah v skladu s členom 9 Uredbe (EU) 2019/1020. Urad za UI zagotavlja usklajevalno podporo za skupne preiskave.

12. Brez poseganja v pooblastila na podlagi Uredbe (EU) 2019/1020 ter kadar je to ustrezno in omejeno na to, kar je potrebno za izpolnjevanje njihovih nalog, ponudniki organom za nadzor trga omogočijo polni dostop do dokumentacije ter naborov učnih, testnih in validacijskih podatkov, ki se uporabljajo za razvoj visokotveganih sistemov UI, vključno z vmesniki za aplikacijsko programiranje (API) ali drugimi ustreznimi tehničnimi sredstvi in orodji, ki omogočajo oddaljeni dostop, kadar je to primerno in ob upoštevanju varnostnih zaščitnih ukrepov.
13. Organom za nadzor trga se dostop do izvirne kode visokotvegane sistema UI odobri na podlagi obrazložene zahteve in samo, če sta izpolnjena oba naslednja pogoja:
- (a) dostop do izvirne kode je potreben za oceno skladnosti visokotvegane sistema UI z zahtevami iz poglavja III, oddelek 2, in
 - (b) postopki testiranja ali revizije in preverjanja na podlagi podatkov in dokumentacije, ki jih je predložil ponudnik, so bili izčrpani ali so se izkazali za nezadostne.
14. Vse informacije ali dokumentacija, ki jih pridobijo organi za nadzor trga, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 75

Medsebojna pomoč, nadzor trga in nadzor sistemov UI za splošne namene

1. Kadar sistem UI temelji na modelu UI za splošne namene ter model in sistem razvije isti ponudnik, ima Urad za UI pooblastila za spremljanje in nadzor skladnosti tega sistema UI z obveznostmi iz te uredbe. Urad za UI ima za izvajanje svojih nalog spremljanja in nadzora vsa pooblastila organa za nadzor trga iz tega oddelka in Uredbe (EU) 2019/1020.
2. Kadar imajo ustrezni organi za nadzor trga zadosten razlog, da sisteme UI za splošne namene, ki jih lahko uvajalci neposredno uporabljajo za vsaj en namen, ki je na podlagi te uredbe razvrščen kot veliko tveganje, štejejo za neskladne z zahtevami iz te uredbe, pri izvajanju ocen skladnosti sodelujejo z Uradom za UI ter o tem ustrezno obvestijo Odbor in druge organe za nadzor trga.

3. Kadar organ za nadzor trga ne more zaključiti preiskave visokotveganega sistema UI, ker ne more dostopati do nekaterih informacij, povezanih z modelom UI za splošne namene, čeprav si je ustrezno prizadeval, da bi jih pridobil, lahko Uradu za UI predloži obrazloženo zahtevo, na podlagi katere se zagotovi dostop do teh informacij. V tem primeru Urad za UI organu prosilcu brez odlašanja, v vsakem primeru pa v 30 dneh, zagotovi vse informacije, za katere meni, da so pomembne za ugotovitev, ali je visokotvegani sistem UI neskladen. Organi za nadzor trga zagotavljajo zaupnost informacij, ki jih pridobijo v skladu s členom 78 te uredbe. Smiselno se uporablja postopek iz poglavja VI Uredbe (EU) 2019/1020.

Člen 76

Nadzor testiranja v realnih razmerah s strani organov za nadzor trga

1. Organi za nadzor trga imajo pristojnosti in pooblastila za zagotavljanje, da je testiranje v realnih razmerah skladno s to uredbo.
2. Kadar se testiranje v realnih razmerah izvaja za sisteme UI, ki se nadzorujejo v regulativnem peskovniku za UI na podlagi člena 58, organi za nadzor trga skladnost s členom 60 preverijo v okviru svoje nadzorne vloge za regulativni peskovnik za UI. Ti organi lahko po potrebi dovolijo, da ponudnik ali potencialni ponudnik opravi testiranje v realnih razmerah z odstopanjem od pogojev iz člena 60(4), točki (f) in (g).

3. Kadar potencialni ponudnik, ponudnik ali katera koli tretja oseba obvesti organ za nadzor trga o resnem incidentu ali ima druge razloge za domnevo, da pogoji iz členov 60 in 61 niso izpolnjeni, lahko na svojem ozemlju sprejme katero koli od naslednjih odločitev:
- (a) začasno ali dokončno ustavi testiranje v realnih razmerah;
 - (b) od ponudnika ali potencialnega ponudnika in uvajalca ali potencialnega uvajalca zahteva, da spremenijo katerega od vidikov testiranja v realnih razmerah.
4. Kadar organ za nadzor trga sprejme odločitev iz odstavka 3 tega člena ali izda ugovor v smislu člena 60(4), točka (b), se v odločitvi ali ugovoru navedejo razlogi zanj ali zanjo ter kako lahko ponudnik ali potencialni ponudnik izpodbija odločitev ali ugovor.
5. Kadar je ustrezno, kadar organ za nadzor trga sprejme odločitev iz odstavka 3, razloge zanjo sporoči organom za nadzor trga iz drugih držav članic, v katerih je bil sistem UI testiran v skladu z načrtom za testiranje.

Člen 77

Pooblastila organov, pristojnih za varstvo temeljnih pravic

1. Nacionalni javni organi ali telesa, ki nadzorujejo ali uveljavljajo spoštovanje obveznosti na podlagi prava Unije o varstvu temeljnih pravic, vključno s pravico do nediskriminacije, so v zvezi z uporabo visokotveganih sistemov UI iz Priloge III pooblašчени, da zahtevajo vso dokumentacijo, ustvarjeno ali hranjeno na podlagi te uredbe, in da v dostopnem jeziku in obliki dostopajo do nje, kadar je dostop do navedene dokumentacije potreben za učinkovito izvrševanje njihovih pooblastil v mejah njihove jurisdikcije. Zadevni javni organ ali telo o vsaki taki zahtevi obvesti organ za nadzor trga zadevne države članice.
2. Vsaka država članica do ... [tri mesece od začetka veljavnosti te uredbe] določi javne organe ali telesa iz odstavka 1 in seznam teh organov ali teles objavi. Države članice o seznamu uradno obvestijo Komisijo in druge države članice ter seznam redno posodablajo.
3. Kadar dokumentacija iz odstavka 1 ne zadošča za ugotovitev, ali je prišlo do kršitve obveznosti na podlagi prava Unije o varstvu temeljnih pravic, lahko javni organ ali telo iz odstavka 1 na podlagi obrazložene zahteve od organa za nadzor trga zahteva, da organizira testiranje visokotvegane sistema UI s tehničnimi sredstvi. Organ za nadzor trga v razumnem času po prejemu zahteve organizira testiranje v tesnem sodelovanju z javnim organom ali telesom, ki je vložilo zahtevo.

4. Vse informacije ali dokumentacija, ki jo nacionalni javni organi ali telesa iz odstavka 1 tega člena pridobijo na podlagi tega člena, se obravnavajo v skladu z obveznostmi glede zaupnosti iz člena 78.

Člen 78

Zaupnost

1. Komisija, organi za nadzor trga in priglašeni organi ter vse druge fizične ali pravne osebe, ki sodelujejo pri uporabi te uredbe, v skladu s pravom Unije ali nacionalnim pravom spoštujejo zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog in dejavnosti, tako da varujejo zlasti:
 - (a) pravice intelektualne lastnine in zaupne poslovne informacije ali poslovne skrivnosti fizične ali pravne osebe, vključno z izvirno kodo, razen v primerih iz člena 5 Direktive (EU) 2016/943 Evropskega parlamenta in Sveta⁵⁷;
 - (b) učinkovito izvajanje te uredbe, zlasti za namene inšpekcijskih pregledov, preiskav ali revizij;
 - (c) javne interese in interese nacionalne varnosti;
 - (d) izvedbo kazenskih ali upravnih postopkov;

⁵⁷ Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritnega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (UL L 157, 15.6.2016, str. 1).

- (e) podatke, ki so tajni na podlagi prava Unije ali nacionalnega prava.
2. Organi, ki sodelujejo pri uporabi te uredbe na podlagi odstavka 1, zahtevajo samo podatke, ki so nujno potrebni za oceno tveganja, ki ga predstavljajo sistemi UI, in za izvajanje svojih pooblastil v skladu s to uredbo in Uredbo (EU) 2019/1020. V skladu z veljavnim pravom Unije ali nacionalnim pravom uvedejo ustrezne in učinkovite ukrepe za kibernetško varnost, da zaščitijo varnost in zaupnost pridobljenih informacij in podatkov, ter zbrane podatke izbrišejo takoj, ko niso več potrebni za namen, za katerega so bili pridobljeni.
3. Brez poseganja v odstavka 1 in 2 se informacije, ki se zaupno izmenjujejo med pristojnimi nacionalnimi organi ali med pristojnimi nacionalnimi organi in Komisijo, ne razkrijejo brez predhodnega posvetovanja z izvirnim pristojnim nacionalnim organom in uvajalcem, kadar visokotvegane sisteme UI iz Priloge III, točke 1, 6 ali 7, uporabljajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi mejne kontrole, organi, pristojni za priseljevanje, ali azilni organi, kadar bi tako razkritje ogrozilo javne in nacionalne varnostne interese. Ta izmenjava informacij ne zajema občutljivih operativnih podatkov v zvezi z dejavnostmi organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organov mejne kontrole in organov, pristojnih za priseljevanje, ali azilnih organov.

Kadar so organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, organi, pristojni za priseljevanje, ali azilni organi ponudniki visokotveganih sistemov UI iz Priloge III, točke 1, 6 ali 7, ostane tehnična dokumentacija iz Priloge IV v prostorih teh organov. Ti organi zagotovijo, da lahko organi za nadzor trga iz člena 74(8) in (9), kot je ustrezno, na zahtevo nemudoma dostopajo do dokumentacije ali pridobijo njeno kopijo. Dostop do te dokumentacije ali njene kopije je dovoljen samo osebu organa za nadzor trga, ki ima ustrezno stopnjo varnostnega preverjanja.

4. Odstavki 1, 2 in 3 ne vplivajo na pravice ali obveznosti Komisije, držav članic in njihovih zadevnih organov ter priglašeni organov v zvezi z izmenjavo informacij in razširjanjem opozoril, tudi v okviru čezmejnega sodelovanja, niti ne vplivajo na obveznosti zadevnih strani, da zagotovijo informacije na podlagi kazenskega prava držav članic.
5. Komisija in države članice lahko po potrebi in v skladu z ustreznimi določbami mednarodnih in trgovinskih sporazumov zaupne informacije izmenjajo z regulativnimi organi tretjih držav, s katerimi so sklenile dvostranske ali večstranske dogovore o zaupnosti, ki zagotavljajo ustrezno raven zaupnosti.

Člen 79

Nacionalni postopek za obravnavo sistemov UI, ki predstavljajo tveganje

1. Sistemi UI, ki predstavljajo tveganje, se štejejo za „proizvod, ki predstavlja tveganje“, kot je opredeljen v členu 3, točka 19, Uredbe (EU) 2019/1020, če predstavljajo tveganje za zdravje, varnost ali temeljne pravice oseb.

2. Kadar ima organ za nadzor trga države članice zadosten razlog za domnevo, da sistem UI predstavlja tveganje iz odstavka 1 tega člena, izvede ocenjevanje skladnosti zadevnega sistema UI z vsemi zahtevami in obveznostmi iz te uredbe. Posebno pozornost nameni sistemom UI, ki predstavljajo tveganje za ranljive skupine. Kadar so ugotovljena tveganja za temeljne pravice, organ za nadzor trga obvesti tudi ustrezne nacionalne javne organe ali telesa iz člena 77(1) in z njimi polno sodeluje. Zadevni operaterji po potrebi sodelujejo z organom za nadzor trga in drugimi nacionalnimi javnimi organi ali telesi iz člena 77(1).

Kadar organ za nadzor trga sam ali, kadar je ustrezno, v sodelovanju z nacionalnim javnim organom iz člena 77(1) med navedenim ocenjevanjem ugotovi, da sistem UI ni skladen z zahtevami in obveznostmi iz te uredbe, od zadevnega operaterja brez nepotrebnega odlašanja zahteva, da sprejme vse ustrezne popravne ukrepe, da zagotovi skladnost sistema UI, ga umakne s trga ali odpokliče v roku, ki ga lahko določi organ za nadzor trga, v vsakem primeru pa najpozneje v 15 delovnih dneh ali kot je določeno v ustrezni harmonizacijski zakonodaji Unije.

Organ za nadzor trga o tem obvesti zadevni priglašeni organ. Za ukrepe iz drugega pododstavka tega odstavka se uporablja člen 18 Uredbe (EU) 2019/1020.

3. Kadar organ za nadzor trga meni, da neskladnost ni omejena na njegovo nacionalno ozemlje, Komisijo in druge države članice brez nepotrebnega odlašanja obvesti o rezultatih ocenjevanja in ukrepih, ki jih je zahteval od operaterja.
4. Operater zagotovi sprejetje vseh ustreznih popravnih ukrepov glede vseh zadevnih sistemov UI, katerih dostopnost je omogočil na trgu Unije.
5. Kadar operater sistema UI ne sprejme ustreznih popravnih ukrepov v roku iz odstavka 2, organ za nadzor trga sprejme vse ustrezne začasne ukrepe za prepoved ali omejitev dostopnosti sistema UI na svojem nacionalnem trgu ali njegovega dajanja v uporabo, za umik proizvoda ali samostojnega sistema UI z navedenega trga ali za njegov odpoklic. Zadevni organ brez nepotrebnega odlašanja uradno obvesti Komisijo in druge države članice o teh ukrepih.
6. Uradno obvestilo iz odstavka 5 vsebuje vse razpoložljive podrobnosti, zlasti informacije, potrebne za identifikacijo neskladnega sistema UI, poreklo sistema UI in dobavno verigo, naravo domnevne neskladnosti in tveganja, naravo in trajanje sprejetih nacionalnih ukrepov ter argumente zadevnega operaterja. Organi za nadzor trga zlasti navedejo, ali je neskladnost posledica enega ali več naslednjih elementov:
 - (a) neupoštevanja prepovedi praks UI iz člena 5;
 - (b) neizpolnjevanja zahtev iz poglavja III, oddelek 2, s strani visokotveganega sistema UI;

- (c) pomanjkljivosti harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41, na katerih temelji domneva o skladnosti;
 - (d) neskladnosti s členom 50.
7. Organi za nadzor trga, ki niso organi za nadzor trga države članice, ki je začela postopek, brez nepotrebnega odlašanja obvestijo Komisijo in druge države članice o vseh sprejetih ukrepih in vseh dodatnih informacijah, ki so jim na voljo v zvezi z neskladnostjo zadevnega sistema UI, v primeru nestrinjanja s priglašenim nacionalnim ukrepom pa tudi o svojih ugovorih.
8. Kadar organ za nadzor trga države članice ali Komisija v treh mesecih po prejemu uradnega obvestila iz odstavka 5 ne poda ugovora glede začasnega ukrepa, ki ga je sprejel organ za nadzor trga druge države članice, se šteje, da je ukrep upravičen. To ne posega v postopkovne pravice zadevnega operaterja v skladu s členom 18 Uredbe (EU) 2019/1020. Trimesečno obdobje iz tega odstavka se skrajša na 30 dni v primeru neupoštevanja prepovedi praks UI iz člena 5 te uredbe.
9. Organi za nadzor trga zagotovijo, da so ustrezni omejevalni ukrepi v zvezi z zadevnim proizvodom ali sistemom UI, kot je umik proizvoda ali sistema UI s trga, sprejeti brez nepotrebnega odlašanja.

Člen 80

Postopek za obravnavo sistemov UI, ki jih je ponudnik v skladu s Prilogo III razvrstil kot sisteme UI brez visokega tveganja

1. Kadar ima organ za nadzor trga zadosten razlog za domnevo, da je sistem UI, ki ga je ponudnik na podlagi člena 6(3) razvrstil kot sistem UI, ki ni visokotvegan, dejansko visokotvegani sistem UI, izvede ocenjevanje zadevnega sistema UI z vidika njegove razvrstitve kot visokotveganega sistema UI na podlagi pogojev iz člena 6(3) in smernic Komisije.
2. Kadar organ za nadzor trga med navedenim ocenjevanjem ugotovi, da gre za visokotvegani sistem UI, od zadevnega ponudnika brez nepotrebnega odlašanja zahteva, da sprejme vse potrebne ukrepe za uskladitev sistema UI z zahtevami in obveznostmi iz te uredbe ter da sprejme ustrezne popravne ukrepe v roku, ki ga lahko določi organ za nadzor trga.
3. Kadar organ za nadzor trga meni, da uporaba zadevnega sistema UI ni omejena na njegovo nacionalno ozemlje, Komisijo in druge države članice brez nepotrebnega odlašanja obvesti o rezultatih ocenjevanja in ukrepih, ki jih je zahteval od ponudnika.

4. Ponudnik zagotovi sprejetje vseh potrebnih ukrepov za uskladitev sistema UI z zahtevami in obveznostmi iz te uredbe. Kadar ponudnik zadevnega sistema UI v roku iz odstavka 2 tega člena ne uskladi sistema UI z zahtevami in obveznostmi, se ponudniku naložijo globe v skladu s členom 99.
5. Ponudnik zagotovi sprejetje vseh ustreznih popravnih ukrepov glede vseh zadevnih sistemov UI, katerih dostopnost je omogočil na trgu Unije.
6. Kadar ponudnik zadevnega sistema UI ne sprejme ustreznih popravnih ukrepov v roku iz odstavka 2 tega člena, se uporablja člen 79(5) do (9).
7. Kadar organ za nadzor trga med ocenjevanjem na podlagi odstavka 1 tega člena ugotovi, da je ponudnik sistem UI napačno razvrstil kot sistem UI, ki ni visokotvegan, da bi se izognil uporabi zahtev iz poglavja III, oddelek 2, se ponudniku naložijo globe v skladu s členom 99.
8. Organi za nadzor trga lahko pri izvajanju svojih pooblastil za spremljanje uporabe tega člena in v skladu s členom 11 Uredbe (EU) 2019/1020 izvajajo ustrezne preglede, pri čemer upoštevajo zlasti informacije, shranjene v podatkovni zbirki EU iz člena 71 te uredbe.

Člen 81
Zaščitni postopek Unije

1. Kadar organ za nadzor trga države članice v treh mesecih od prejema uradnega obvestila iz člena 79(5) ali v 30 dneh v primeru neupoštevanja prepovedi praks UI iz člena 5 poda ugovor proti ukrepu, ki ga je sprejel drug organ za nadzor trga, ali kadar Komisija meni, da je ukrep v nasprotju s pravom Unije, se Komisija brez nepotrebnega odlašanja posvetuje z organom za nadzor trga zadevne države članice in operaterjem ali operaterji ter oceni nacionalni ukrep. Komisija na podlagi rezultatov navedenega ocenjevanja v šestih mesecih ali v 60 dneh v primeru neupoštevanja prepovedi praks UI iz člena 5 od uradnega obvestila iz člena 79(5) odloči, ali je nacionalni ukrep upravičen, in o taki odločitvi uradno obvesti organ za nadzor trga zadevne države članice. Komisija o svoji odločitvi tudi obvesti vse druge organe za nadzor trga.
2. Kadar Komisija meni, da je ukrep, ki ga je sprejela zadevna država članica, upravičen, vse države članice zagotovijo, da v zvezi z zadevnim sistemom UI sprejmejo ustrezne omejevalne ukrepe, kot je zahteva za umik sistema UI z njihovega trga brez nepotrebnega odlašanja, in o tem obvestijo Komisijo. Kadar Komisija meni, da nacionalni ukrep ni upravičen, zadevna država članica ukrep prekliče in o tem obvesti Komisijo.

3. Kadar se nacionalni ukrep šteje za upravičenega, neskladnost sistema UI pa je pripisana pomanjkljivosti harmoniziranih standardov ali skupnih specifikacij iz členov 40 in 41 te uredbe, Komisija uporabi postopek iz člena 11 Uredbe (EU) št. 1025/2012.

Člen 82

Skladni sistemi UI, ki predstavljajo tveganje

1. Kadar organ za nadzor trga države članice po opravljenem ocenjevanju iz člena 79 in posvetovanju z zadevnim nacionalnim javnim organom iz člena 77(1) ugotovi, da visokotvegani sistem UI, ki je skladen s to uredbo, kljub temu predstavlja tveganje za zdravje ali varnost oseb, temeljne pravice ali druge vidike zaščite javnih interesov, od zadevnega operaterja zahteva, da brez nepotrebnega odlašanja v roku, ki ga lahko določi organ za nadzor trga, sprejme vse ustrezne ukrepe, s katerimi zagotovi, da zadevni sistem UI, ko je dan na trg ali v uporabo, tega tveganja ne predstavlja več.
2. Ponudnik ali drugi zadevni operater zagotovi sprejetje popravnih ukrepov glede vseh zadevnih sistemov UI, katerih dostopnost na trgu Unije je omogočil, v roku, ki ga določi organ za nadzor trga države članice iz odstavka 1.

3. Države članice o ugotovitvi na podlagi odstavka 1 nemudoma obvestijo Komisijo in druge države članice. Navedene informacije vključujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo zadevnega sistema UI, poreklo in dobavno verigo sistema UI, naravo zadevnega tveganja ter naravo in trajanje sprejetih nacionalnih ukrepov.
4. Komisija se brez nepotrebnega odlašanja posvetuje z zadevnimi državami članicami in ustreznimi operaterji ter oceni sprejete nacionalne ukrepe. Na podlagi rezultatov navedenega ocenjevanja odloči, ali je ukrep upravičen, in po potrebi predlaga druge ustrezne ukrepe.
5. Komisija svojo odločitev nemudoma sporoči zadevnim državam članicam in ustreznim operaterjem. Obvesti tudi vse druge države članice.

Člen 83

Formalna neskladnost

1. Kadar organ za nadzor trga države članice ugotovi eno od naslednjih dejstev, od zadevnega ponudnika zahteva, naj zadevno neskladnost odpravi v roku, ki ga lahko določi organ za nadzor trga:
 - (a) oznaka CE ni nameščena v skladu s členom 48;
 - (b) oznaka CE ni bila nameščena;
 - (c) EU izjava o skladnosti iz člena 47 ni pripravljena;

- (d) EU izjava o skladnosti iz člena 47 ni pravilno pripravljena;
 - (e) registracija v podatkovni zbirki EU iz člena 71 ni bila opravljena;
 - (f) kadar je ustrezno, pooblaščen predstavniki ni bil imenovan;
 - (g) tehnična dokumentacija ni na voljo.
2. Kadar se neskladnost iz odstavka 1 nadaljuje, organ za nadzor trga zadevne države članice nemudoma sprejme vse ustrezne in sorazmerne ukrepe za to, da se omogočanje dostopnosti visokotveganega sistema UI na trgu omeji ali prepove oziroma da se tak sistem brez odlašanja prekliče ali umakne s trga.

Člen 84

Podporne strukture Unije za testiranje UI

1. Komisija za opravljanje nalog na podlagi člena 21(6) Uredbe (EU) 2019/1020 na področju UI imenuje eno ali več podpornih struktur Unije za testiranje UI.
2. Brez poseganja v naloge iz odstavka 1 podporne strukture Unije za testiranje UI na zahtevo Odbora, Komisije ali organov za nadzor trga zagotavljajo tudi neodvisno tehnično ali znanstveno svetovanje.

ODDELEK 4

PРАВNA SREDSTVA

Člen 85

Pravica do vložitve pritožbe pri organu za nadzor trga

Brez poseganja v druga upravna ali pravna sredstva lahko pritožbe pri ustreznem organu za nadzor trga vloži vsaka fizična ali pravna oseba, ki utemeljeno meni, da je prišlo do kršitve določb te uredbe.

V skladu z Uredbo (EU) 2019/1020 se pritožbe upoštevajo za namen izvajanja dejavnosti nadzora trga in se obravnavajo v skladu z namenskimi postopki, ki jih za to vzpostavijo organi za nadzor trga.

Člen 86

Pravica do obrazložitve postopka odločanja za posamične primere

1. Vsaka prizadeta oseba, za katero velja odločitev, ki jo uvajalec sprejme na podlagi izhodnih podatkov visokotveganega sistema UI iz Priloge III, razen sistemov iz točke 2 Priloge III, in ki ima pravne učinke ali na to osebo podobno znatno vpliva na način, ki ima po njenem mnenju negativne učinke na njeno zdravje, varnost in temeljne pravice, ima pravico od uvajalca pridobiti jasna in smiselna pojasnila o vlogi sistema UI v postopku odločanja in glavnih elementih sprejete odločitve.

2. Odstavek 1 se ne uporablja za uporabo sistemov UI, za katere izjeme od obveznosti iz navedenega odstavka ali omejitve teh obveznosti izhajajo iz prava Unije ali nacionalnega prava v skladu s pravom Unije.
3. Ta člen se uporablja le, če pravica iz odstavka 1 še ni drugje določena na podlagi prava Unije.

Člen 87

Prijava kršitev in zaščita prijaviteljev

Za prijavo kršitev te uredbe in zaščito oseb, ki prijavijo take kršitve, se uporablja Direktiva (EU) 2019/1937.

ODDELEK 5

NADZOR, PREISKOVANJE, IZVRŠEVANJE IN SPREMLJANJE V ZVEZI S PONUDNIKI MODELOV UI ZA SPLOŠNE NAMENE

Člen 88

Izvrševanje obveznosti ponudnikov modelov UI za splošne namene

1. Komisija ima izključne pristojnosti za nadzor in izvrševanje poglavja V, pri čemer upošteva procesna jamstva na podlagi člena 94. Izvajanje teh nalog zaupa Uradu za UI, brez poseganja v organizacijska pooblastila Komisije ter delitev pristojnosti med državami članicami in Unijo na podlagi Pogodb.

2. Brez poseganja v člen 75(3) lahko organi za nadzor trga od Komisije zahtevajo, da izvaja pooblastila iz tega oddelka, kadar je to potrebno in sorazmerno za pomoč pri izpolnjevanju njihovih nalog na podlagi te uredbe.

Člen 89

Ukrepi spremljanja

1. Urad za UI lahko za namen opravljanja nalog, ki jih ima na podlagi tega oddelka, sprejme ukrepe, potrebne za spremljanje učinkovitega izvajanja te uredbe in skladnosti z njo s strani ponudnikov modelov UI za splošne namene, vključno z upoštevanjem odobrenih kodeksov prakse.
2. Ponudniki nižje v verigi imajo pravico vložiti pritožbo o domnevni kršitvi te uredbe. Pritožba mora biti ustrezno obrazložena in vsebuje vsaj:
 - (a) kontaktno točko zadevnega ponudnika modela UI za splošne namene;
 - (b) opis relevantnih dejstev, zadevnih določb te uredbe in razloga, zakaj ponudnik nižje v verigi meni, da je zadevni ponudnik modela UI za splošne namene kršil to uredbo;
 - (c) vse druge informacije, za katere ponudnik nižje v verigi, ki je poslal zahtevo, meni, da so pomembne, po potrebi tudi informacije, ki jih je zbral na lastno pobudo.

Člen 90

Opozorila znanstvenega odbora o sistemskih tveganjih

1. Znanstveni odbor lahko Uradu za UI pošlje kvalificirano opozorilo, kadar ima razlog za sum, da:
 - (a) model UI za splošne namene predstavlja konkretno prepoznavno tveganje na ravni Unije ali
 - (b) model UI za splošne namene izpolnjuje pogoje iz člena 51.
2. Po takem kvalificiranem opozorilu lahko Komisija prek Urada za UI in po obvestitvi Odbora izvaja pooblastila iz tega oddelka, da bi ocenila zadevo. Urad za UI obvesti Odbor o vseh ukrepih v skladu s členi 91 do 94.
3. Kvalificirano opozorilo mora biti ustrezno obrazloženo in vsebuje vsaj:
 - (a) kontaktno točko ponudnika zadevnega modela UI za splošne namene s sistemskim tveganjem;
 - (b) opis relevantnih dejstev in razlogov za obvestilo znanstvenega odbora;
 - (c) vse druge informacije, za katere znanstveni odbor meni, da so pomembne, po potrebi tudi informacije, ki jih je zbral na lastno pobudo.

Člen 91

Pooblastilo za zahtevanje dokumentacije in informacij

1. Komisija lahko od zadevnega ponudnika modela UI za splošne namene zahteva, da predloži dokumentacijo, ki jo je pripravil v skladu s členoma 53 in 55, ali vse dodatne informacije, ki so potrebne za oceno skladnosti ponudnika s to uredbo.
2. Preden se pošlje zahteva za informacije, lahko Urad za UI začne strukturiran dialog s ponudnikom modela UI za splošne namene.
3. Komisija lahko na ustrezno utemeljeno zahtevo znanstvenega odbora ponudniku modela UI za splošne namene pošlje zahtevo za informacije, kadar je dostop do informacij potreben in sorazmeren za izpolnjevanje nalog znanstvenega odbora na podlagi člena 68(2).
4. V zahtevi za informacije se navedeta pravna podlaga in namen zahteve, navedejo se informacije, ki se zahtevajo, določi rok, v katerem je treba informacije predložiti, pa tudi globe iz člena 101 za predložitev nepravilnih, nepopolnih ali zavajajočih informacij.

5. Ponudnik zadevnega modela UI za splošne namene ali njegov zastopnik zagotovi zahtevane informacije. V primeru pravnih oseb, podjetij ali družb ali kadar ponudnik nima pravne osebnosti, zahtevane informacije v imenu zadevnega ponudnika modela UI za splošne namene predložijo osebe, ki so z zakonom ali statutom pooblašcene, da jih zastopajo. Pooblašчени odvetniki lahko predložijo informacije v imenu svojih strank. Stranke so kljub temu v celoti odgovorne, če so predložene informacije nepopolne, napačne ali zavajajoče.

Člen 92

Pooblastilo za izvajanje ocenjevanja

1. Urad za UI lahko po posvetovanju z Odborom izvede ocenjevanje zadevnega modela UI za splošne namene, da:
 - (a) oceni, ali ponudnik izpolnjuje obveznosti iz te uredbe, kadar informacije, zbrane na podlagi člena 91, niso zadostne, ali
 - (b) razišče sistemska tveganja modelov UI za splošne namene s sistemskim tveganjem na ravni Unije, zlasti na podlagi kvalificiranega obvestila znanstvenega odbora v skladu s členom 90(1), točka (a).
2. Komisija se lahko odloči, da imenuje neodvisne strokovnjake, tudi iz znanstvenega odbora, ustanovljenega na podlagi člena 68, da v njenem imenu izvedejo ocenjevanje. Neodvisni strokovnjaki, imenovani za to nalogo, morajo izpolnjevati merila iz člena 68(2).

3. Za namene odstavka 1 lahko Komisija zahteva dostop do zadevnega modela UI za splošne namene prek API ali drugih ustreznih tehničnih sredstev in orodij, vključno z izvorno kodo.
4. V zahtevi za dostop se navedejo pravna podlaga, namen zahteve in razlogi zanjo ter določi rok, v katerem je treba zagotoviti dostop, pa tudi globe iz člena 101, če se dostop ne zagotovi.
5. Zadevni ponudnik modela UI za splošne namene ali njegov predstavnik zagotovi zahtevane informacije. V primeru pravnih oseb pa podjetja ali družbe ali, kadar ponudnik nima pravne osebnosti, osebe, ki so z zakonom ali statutom pooblaščne, da jih zastopajo, zagotovijo zahtevani dostop v imenu zadevnega ponudnika modela UI za splošne namene.
6. Komisija sprejme izvedbene akte, v katerih določi podrobnosti in pogoje ocenjevanja, vključno s podrobnostmi glede vključevanja neodvisnih strokovnjakov, ter postopek za njihov izbor. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).
7. Preden Urad za UI zaprosi za dostop do zadevnega modela UI za splošne namene, lahko začne strukturiran dialog s ponudnikom modela UI za splošne namene, da bi zbral več informacij o notranjem testiranju modela, notranjih zaščitnih ukrepih za preprečevanje sistemskih tveganj ter drugih notranjih postopkih in ukrepih, ki jih je ponudnik sprejel za zmanjšanje takih tveganj.

Člen 93

Pooblastilo za zahtevanje ukrepov

1. Kadar je to potrebno in primerno, lahko Komisija od ponudnikov zahteva, da:
 - (a) sprejmejo ustrezne ukrepe za izpolnjevanje obveznosti iz členov 53 in 54;
 - (b) izvedejo ukrepe za zmanjšanje tveganj, kadar je ocena, izvedena v skladu s členom 92, vzbudila resne in utemeljene pomisleke glede sistemskega tveganja na ravni Unije;
 - (c) omejijo omogočanje dostopnosti modela na trgu, ga umaknejo s trga ali odpokličejo.
2. Preden se zahteva ukrep, lahko Urad za UI začne strukturiran dialog s ponudnikom modela UI za splošne namene.
3. Če ponudnik modela UI za splošne namene s sistemskim tveganjem med strukturiranim dialogom iz odstavka 2 ponudi zaveze za izvajanje ukrepov za zmanjšanje sistemskih tveganj na ravni Unije, lahko Komisija s sklepom določi, da so te zaveze zavezujoče, in izjavi, da ni nadaljnjih razlogov za ukrepanje.

Člen 94

Postopkovne pravice gospodarskih subjektov v zvezi z modelom UI za splošne namene

Člen 18 Uredbe (EU) 2019/1020 se smiselno uporablja za ponudnike modela UI za splošne namene brez poseganja v bolj specifične postopkovne pravice iz te uredbe.

Poglavje X

Kodeksi ravnanja in smernice

Člen 95

Kodeksi ravnanja za prostovoljno uporabo posebnih zahtev

1. Urad za UI in države članice spodbujajo in olajšujejo pripravo kodeksov ravnanja, vključno s pripadajočimi mehanizmi upravljanja, namenjenih spodbujanju prostovoljne uporabe nekaterih ali vseh zahtev iz poglavja III, oddelek 2, za sisteme UI, ki niso visokotvegani sistemi UI, pri čemer upoštevajo razpoložljive tehnične rešitve in najboljše prakse v tem sektorju, ki omogočajo uporabo takih zahtev.

2. Urad za UI in države članice olajšujejo pripravo kodeksov ravnanja v zvezi s prostovoljno uporabo posebnih zahtev za vse sisteme UI, tudi s strani uvajalcev, na podlagi jasnih ciljev in ključnih kazalnikov uspešnosti za merjenje doseganja teh ciljev, vključno z elementi, kot so med drugim:
- (a) veljavni elementi, določeni v etičnih smernicah Unije za zaupanja vredno umetno inteligenco;
 - (b) ocenjevanje in zmanjšanje vpliva sistemov UI na okoljsko trajnostnost, tudi v zvezi z načrtovanjem in tehnikami energetske učinkovitosti za učinkovito snovanje, učenje in uporabo UI;
 - (c) spodbujanje pismenosti na področju UI, zlasti oseb, ki se ukvarjajo z razvijanjem, delovanjem in uporabo UI;
 - (d) spodbujanje vključujoče in raznolike zasnove sistemov UI, tudi z ustanovitvijo vključujočih in raznolikih skupin razvijalcev ter spodbujanjem vključevanja deležnikov v ta proces;
 - (e) ocenjevanje in preprečevanje negativnega vpliva sistemov UI na ranljive osebe ali skupine ranljivih oseb, tudi kar zadeva dostopnost za invalide, pa tudi na enakost spolov.

3. Kodekse ravnanja lahko pripravijo posamezni ponudniki ali uvajalci sistemov UI ali organizacije, ki jih zastopajo, ali oboji, pri tem pa lahko sodelujejo vsi deležniki ter njihove predstavniške organizacije, vključno z organizacijami civilne družbe in akademskimi krogi. Kodeksi ravnanja lahko zajemajo enega ali več sistemov UI ob upoštevanju podobnosti predvidenega namena zadevnih sistemov.
4. Urad za UI in države članice pri spodbujanju in olajševanju priprave kodeksov ravnanja upoštevajo posebne interese in potrebe MSP, vključno z zagonskimi podjetji.

Člen 96

Smernice Komisije za izvajanje te uredbe

1. Komisija pripravi smernice za praktično izvajanje te uredbe, zlasti glede:
 - (a) izpolnjevanja zahtev in obveznosti iz členov 8 do 15 in člena 25;
 - (b) prepovedanih praks iz člena 5;
 - (c) praktičnega izvajanja določb v zvezi z bistveno spremembo;
 - (d) praktičnega izvajanja obveznosti glede preglednosti iz člena 50;

- (e) podrobnih informacij o razmerju te uredbe do harmonizacijske zakonodaje Unije iz Priloge I ter drugega ustreznega prava Unije, tudi kar zadeva doslednost pri njihovem izvrševanju;
- (f) uporabe opredelitve sistema UI iz člena 3, točka 1.

Komisija pri izdaji takih smernic posebno pozornost nameni potrebam MSP, vključno z zagonskimi podjetji, ter lokalnih javnih organov in sektorjev, na katere bo ta uredba najverjetneje vplivala.

Smernice iz prvega pododstavka tega odstavka ustrezno upoštevajo splošno priznane najsodobnejše tehnološke dosežke na področju UI ter ustrezne harmonizirane standarde in skupne specifikacije iz členov 40 in 41 oziroma harmonizirane standarde ali tehnične specifikacije, ki so določeni na podlagi harmonizacijskega prava Unije.

2. Komisija na zahtevo držav članic ali Urada za UI ali na lastno pobudo po potrebi posodobi že sprejete smernice.

Poglavje XI

Prenos pooblastil in postopek v odboru

Člen 97

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.
2. Pooblastilo za sprejemanje delegiranih aktov iz člena 6(6) in (7), člena 7(1) in (3), člena 11(3), člena 43(5) in (6), člena 47(5), člena 51(3), člena 52(4) ter člena 53(5) in (6) se prenese na Komisijo za obdobje pet let od ... [datum začetka veljavnosti te uredbe]. Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega obdobja. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.
3. Prenos pooblastila iz člena 6(6) in (7), člena 7(1) in (3), člena 11(3), člena 43(5) in (6), člena 47(5), člena 51(3), člena 52(4) ter člena 53(5) in (6) lahko kadarkoli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.
5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.
6. Delegirani akt, sprejet na podlagi člena 6(6) ali (7), člena 7(1) ali (3), člena 11(3), člena 43(5) ali (6), člena 47(5), člena 51(3), člena 52(4) ali člena 53(5) ali (6), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku treh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za tri mesece.

Člen 98

Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Poglavje XII

Kazni

Člen 99

Kazni

1. Države članice v skladu s pogoji iz te uredbe določijo pravila o kaznih in drugih izvršilnih ukrepih, ki lahko vključujejo tudi opozorila in nadenarne ukrepe, ki se uporabljajo za kršitve te uredbe s strani operaterjev, ter sprejmejo vse potrebne ukrepe za zagotovitev njihovega pravilnega in učinkovitega izvajanja, pri čemer upoštevajo smernice, ki jih izda Komisija na podlagi člena 96. Te kazni morajo biti učinkovite, sorazmerne in odvračilne. Upoštevajo interese MSP, vključno z zagonskimi podjetji, in njihovo ekonomsko sposobnost.
2. Države članice brez odlašanja in najpozneje do datuma začetka uporabe uradno obvestijo Komisijo o pravilih o kaznih in drugih izvršilnih ukrepih iz odstavka 1 ter o vseh naknadnih spremembah teh pravil.
3. Neupoštevanje prepovedi praks UI iz člena 5 se kaznuje z upravnimi globami v višini do 35 000 000 EUR ali, če je kršitelj podjetje, do 7 % njegovega skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji.

4. Neskladnost s katero koli od naslednjih določb, ki se nanašajo na operaterje in priglašene organe, razen tistih iz člena 5, se kaznuje z upravnimi globami v višini do 15 000 000 EUR ali, če je kršitelj podjetje, do 3 % njegovega skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji:
- (a) obveznosti ponudnikov na podlagi člena 16;
 - (b) obveznosti pooblaščenih zastopnikov na podlagi člena 22;
 - (c) obveznosti uvoznikov na podlagi člena 23;
 - (d) obveznosti distributerjev na podlagi člena 24;
 - (e) obveznosti uvajalcev na podlagi člena 26;
 - (f) zahteve in obveznosti priglašanih organov na podlagi člena 31, člena 33(1), (3) in (4) ali člena 34;
 - (g) obveznosti ponudnikov in uvajalcev glede preglednosti na podlagi člena 50.
5. Če se priglašeni organ ali pristojni nacionalni organ v odgovor na zahtevo predložijo nepravilne, nepopolne ali zavajajoče informacije, se izrečejo upravne globe do 7 500 000 EUR ali, če je kršitelj podjetje, do 1 % njegovega skupnega svetovnega letnega prometa za preteklo poslovno leto, odvisno od tega, kateri znesek je višji.
6. V primeru MSP, vključno z zagonskimi podjetji, višina vsake globe iz tega člena ne presega višine odstotkov ali zneska iz odstavkov 3, 4 in 5, odvisno od tega, kateri znesek je nižji.

7. Pri odločanju o naložitvi upravne globe in o znesku upravne globe v vsakem posameznem primeru se upoštevajo vse zadevne okoliščine konkretnega primera, po potrebi pa tudi naslednje:
- (a) vrsta, resnost in trajanje kršitve ter njene posledice, pri čemer se upoštevajo namen sistema UI ter po potrebi število prizadetih oseb in raven škode, ki so jo utrpeli;
 - (b) ali so drugi organi za nadzor trga že naložili upravne globe istemu operaterju za isto kršitev;
 - (c) ali so drugi organi istemu operaterju že naložili upravne globe za kršitve drugega prava Unije ali nacionalnega prava, kadar so take kršitve posledica iste dejavnosti ali opustitve dejanja, ki pomeni zadevno kršitev te uredbe;
 - (d) velikost, letni promet in tržni delež operaterja, ki je storil kršitev;
 - (e) morebitni drugi obteževalni ali olajševalni dejavniki v zvezi z okoliščinami primera, kot so pridobljene finančne koristi ali preprečene izgube, ki neposredno ali posredno izhajajo iz kršitve;
 - (f) stopnja sodelovanja z nacionalnimi pristojnimi organi za odpravo kršitve in zmanjšanje morebitnih škodljivih učinkov kršitve;

- (g) stopnja odgovornosti operaterja ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih izvaja;
 - (h) način, na katerega so nacionalni pristojni organi seznanjeni s kršitvijo, zlasti pa, ali in v kakšnem obsegu operater kršitev priglasil;
 - (i) ali je kršitev naklepna ali posledica malomarnosti;
 - (j) ukrepi, ki jih operater sprejme za zmanjšanje škode, ki so jo utrpeli prizadete osebe.
8. Vsaka država članica določi pravila o tem, v kolikšni meri se lahko javnim organom in telesom s sedežem v zadevni državi članici naložijo upravne globe.
9. Glede na pravni sistem držav članic se lahko pravila o upravnih globah uporabljajo tako, da globe naložijo pristojna nacionalna sodišča ali drugi organi, kot velja v teh državah članicah. Uporaba takih pravil v teh državah članicah ima enakovreden učinek.
10. Za izvajanje pooblastil na podlagi tega člena veljajo ustrezna postopkovna jamstva v skladu s pravom Unije in nacionalnim pravom, vključno z učinkovitimi pravnimi sredstvi in ustreznim pravnim postopkom.
11. Države članice Komisiji vsako leto poročajo o upravnih globah, ki so jih v skladu s tem členom naložile v tistem letu, in o vseh povezanih pravnih sporih ali sodnih postopkih.

Člen 100

Upravne globe za institucije, organe, urade in agencije Unije

1. Evropski nadzornik za varstvo podatkov lahko naloži upravne globe institucijam, organom, uradom in agencijam Unije, ki spadajo na področje uporabe te uredbe. Pri odločanju o naložitvi upravne globe in odločanju o znesku upravne globe v vsakem posameznem primeru se upoštevajo vse zadevne okoliščine za konkretno situacijo, ustrezno pa se upošteva tudi naslednje:
 - (a) vrsta, resnost in trajanje kršitve ter njene posledice, pri čemer se upoštevajo namen zadevnega sistema UI ter, kadar je ustrezno, število prizadetih oseb in raven škode, ki so jo utrpeli;
 - (b) stopnja odgovornosti institucije, organa, urada ali agencije Unije, ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih izvaja;
 - (c) ukrepi, ki jih institucija, organ, urad ali agencija Unije sprejme za zmanjšanje škode, ki so jo utrpeli prizadete osebe;
 - (d) obseg sodelovanja z Evropskim nadzornikom za varstvo podatkov za odpravo kršitve in zmanjšanje morebitnih škodljivih učinkov kršitve, vključno z upoštevanjem katerega koli ukrepa, ki ga je Evropski nadzornik za varstvo podatkov predhodno odredil zoper zadevno institucijo, organ, urad ali agencijo Unije v zvezi z isto vsebino;

- (e) vse podobne prejšnje kršitve institucije, organa, urada ali agencije Unije;
 - (f) kako je Evropski nadzornik za varstvo podatkov izvedel za kršitev, zlasti če in v kakšnem obsegu ga je institucija, organ, urad ali agencija Unije uradno obvestila o kršitvi;
 - (g) letni proračun institucije, organa, urada ali agencije Unije.
2. Za neupoštevanje prepovedi praks UI iz člena 5 se kaznuje z upravnimi globami v višini do 1 500 000 EUR.
 3. Neskladnost sistema UI s katerimi koli zahtevami ali obveznostmi iz te uredbe, razen tistih iz člena 5, se kaznuje z upravnimi globami v višini do 750 000 EUR.
 4. Evropski nadzornik za varstvo podatkov pred sprejetjem odločitev na podlagi tega člena instituciji, organu, uradu ali agenciji Unije, zaradi katerih je začel postopek, omogoči, da podajo izjavo o zadevi v zvezi z morebitno kršitvijo. Evropski nadzornik za varstvo podatkov svoje odločitve sprejme zgolj na podlagi elementov in okoliščin, na katere so lahko zadevne strani podale pripombe. Morebitni pritožniki so tesno povezani s postopki.

5. V postopkih se v celoti spoštujejo pravice zadevnih strani do obrambe. Zagotovljena jim je tudi pravica do vpogleda v spis Evropskega nadzornika za varstvo podatkov, pri čemer se upošteva zakonit interes posameznikov ali podjetij za varstvo njihovih osebnih podatkov ali poslovnih skrivnosti.
6. Sredstva, zbrana z naložitvijo glob iz tega člena, pripadajo splošnemu proračunu Unije. Globe ne smejo vplivati na učinkovito delovanje oglobljene institucije, organa, urada ali agencije Unije.
7. Evropski nadzornik za varstvo podatkov Komisijo vsako leto uradno obvesti o upravnih globah, ki jih je naložil na podlagi tega člena, in o vseh pravnih sporih ali sodnih postopkih, ki jih je začel.

Člen 101

Globe, naložene ponudnikom modelov UI za splošne namene

1. Komisija lahko ponudnikom modelov UI za splošne namene naloži globe, ki ne presegajo 3 % njihovega letnega skupnega svetovnega prometa v predhodnem poslovnem letu ali 15 000 000 EUR, odvisno od tega, kateri znesek je višji, če ugotovi, da je ponudnik naklepno ali iz malomarnosti:
 - (a) kršil ustrezne določbe te uredbe;
 - (b) ni izpolnil zahteve za dokumentacijo ali informacije na podlagi člena 91 ali da je naklepno ali iz malomarnosti predložil nepravilne, nepopolne ali zavajajoče informacije;

- (c) ni ravnal v skladu z ukrepom, zahtevanim na podlagi člena 93;
- (d) Komisiji ni omogočil dostopa do modela UI za splošne namene ali modela UI za splošne namene s sistemskim tveganjem, da bi izvedla ocenjevanje na podlagi člena 92.

Pri določanju zneska globe ali periodične denarne kazni se upoštevajo narava, teža in trajanje kršitve, ustrezno pa se upoštevata tudi načeli sorazmernosti in primernosti.

Komisija upošteva tudi zaveze, sprejete v skladu s členom 93(3) ali sprejete v ustreznih kodeksih praksev skladu s členom 56.

- 2. Komisija pred sprejetjem odločitve na podlagi odstavka 1 sporoči svoje predhodne ugotovitve ponudniku modela UI za splošne namene tveganjem in mu da priložnost, da se o njih opredeli.
- 3. Globe, naložene v skladu s tem členom, morajo biti učinkovite, sorazmerne in odvračilne.
- 4. Informacije o globah, naloženih na podlagi tega člena, se po potrebi sporočijo tudi Odboru.
- 5. Sodišče Evropske unije ima neomejeno pristojnost za pregled odločitev Komisije o določitvi globe na podlagi tega člena. Naloženo globo lahko prekliče, zniža ali zviša.

6. Komisija sprejme izvedbene akte, v katerih določi podrobne ureditve in postopkovna jamstva za postopke z vidika morebitnega sprejemanja odločitev na podlagi odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 98(2).

Poglavje XIII

Končne določbe

Člen 102

Sprememba Uredbe (ES) št. 300/2008

V členu 4(3) Uredbe (ES) št. 300/2008 se doda naslednji pododstavek:

„Pri sprejemanju podrobnih ukrepov v zvezi s tehničnimi specifikacijami za varnostno opremo in postopke za njeno odobritev in uporabo v zvezi z umetnointeligentnimi sistemi v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta⁺ se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 103
Sprememba Uredbe (EU) št. 167/2013

V členu 17(5) Uredbe (EU) št. 167/2013 se doda naslednji pododstavek:

„Pri sprejemanju delegiranih aktov na podlagi prvega pododstavka o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta⁺, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 104
Sprememba Uredbe (EU) št. 168/2013

V členu 22(5) Uredbe (EU) št. 168/2013 se doda naslednji pododstavek:

„Pri sprejemanju delegiranih aktov na podlagi prvega pododstavka o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta⁺, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 105
Sprememba Direktive 2014/90/EU

V členu 8 Direktive 2014/90/EU se doda naslednji odstavek:

- „5. Za umetnointeligenčne sisteme, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta^{*,†}, Komisija pri izvajanju svojih dejavnosti na podlagi odstavka 1 ter pri sprejemanju tehničnih specifikacij in standardov preskušanja v skladu z odstavkoma 2 in 3 upošteva zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

[†] UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 106
Sprememba Direktive (EU) 2016/797

V členu 5 Direktive (EU) 2016/797 se doda naslednji odstavek:

- „12. Pri sprejemanju delegiranih aktov na podlagi odstavka 1 in izvedbenih aktov na podlagi odstavka 11 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta^{*,+}, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 107
Sprememba Uredbe (EU) 2018/858

V členu 5 Uredbe (EU) 2018/858 se doda naslednji odstavek:

- „4. „Pri sprejemanju delegiranih aktov na podlagi odstavka 3 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta^{*,+}, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 108
Spremembe Uredbe (EU) 2018/1139

Uredba (EU) 2018/1139 se spremeni:

(1) v členu 17 se doda naslednji odstavek:

„3. „Brez poseganja v odstavek 2 se pri sprejemanju izvedbenih aktov na podlagi odstavka 1 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta^{*,+}, upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“;

(2) v členu 19 se doda naslednji odstavek:

„4. Pri sprejemanju delegiranih aktov na podlagi odstavkov 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/...^{++,} se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

⁺⁺ UL: prosimo, da vstavite številko te uredbe (2021/0106(COD)).

(3) v členu 43 se doda naslednji odstavek:

„4. Pri sprejemanju izvedbenih aktov na podlagi odstavka 1 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/...⁺, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(4) v členu 47 se doda naslednji odstavek:

„3. Pri sprejemanju delegiranih aktov na podlagi odstavkov 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/...⁺, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(5) v členu 57 se doda naslednji pododstavek:

„Pri sprejemanju teh izvedbenih aktov o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/...⁺, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“;

(6) v členu 58 se doda naslednji odstavek:

„3. Pri sprejemanju delegiranih aktov na podlagi odstavkov 1 in 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/...⁺, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.“.

⁺ UL: prosimo, da vstavite številko te uredbe (2021/0106(COD)).

Člen 109
Sprememba Uredbe (EU) 2019/2144

V členu 11 Uredbe (EU) 2019/2144 se doda naslednji odstavek:

- „3. Pri sprejemanju izvedbenih aktov na podlagi odstavka 2 o umetnointeligenčnih sistemih, ki so varnostne komponente v smislu Uredbe (EU) 2024/... Evropskega parlamenta in Sveta^{*,+}, se upoštevajo zahteve iz poglavja III, oddelek 2, navedene uredbe.

* Uredba (EU) 2024/... Evropskega parlamenta in Sveta z dne ... o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

⁺ UL: prosimo, da v besedilo vstavite številko te uredbe (2021/0106(COD)) in dopolnite pripadajočo opombo.

Člen 110
Sprememba Direktive (EU) 2020/1828

V Prilogi I k Direktivi (EU) 2020/1828 Evropskega parlamenta in Sveta⁵⁸ se doda naslednja točka:

„(68) Uredba (EU) 2024/... Evropskega parlamenta in Sveta ...⁺ o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, ..., ELI: ...).“

Člen 111
Sistemi UI, ki so že dani na trg ali v uporabo,
in modeli UI za splošne namene, ki so že dani na trg

1. Brez poseganja v uporabo člena 5, kakor je predvidena v členu 113(3), točka (a), se sistemi UI, ki so komponente obsežnih informacijskih sistemov, vzpostavljenih s pravnimi akti iz Priloge X, in ki so bili dani na trg ali v uporabo pred ... [36 mesecev od datuma začetka veljavnosti te uredbe], uskladijo s to uredbo do 31. decembra 2030.

⁵⁸ Direktiva (EU) 2020/1828 Evropskega parlamenta in Sveta z dne 25. novembra 2020 o zastopniških tožbah za varstvo kolektivnih interesov potrošnikov in razveljavitvi Direktive 2009/22/ES (UL L 409, 4.12.2020, str. 1).

⁺ UL: prosimo, da v besedilo vstavite datum in številko te uredbe (2021/0106(COD)).

Zahteve iz te uredbe se upoštevajo pri ocenjevanju vsakega obsežnega informacijskega sistema, vzpostavljenega s pravnimi akti iz Priloge X, ki ga je treba izvesti, kot je določeno v teh pravnih aktih in kadar se ti pravni akti nadomestijo ali spremenijo.

2. Brez poseganja v uporabo člena 5, kakor je predvidena v členu 113(3), točka (a), se ta uredba uporablja za operaterje visokotveganih sistemov UI, razen sistemov iz odstavka 1 tega člena, ki so bili dani na trg ali v uporabo pred ... [24 mesecev od datuma začetka veljavnosti te uredbe], le, če se je pri navedenih sistemih od navedenega datuma bistveno spremenila njihova zasnova. V vsakem primeru ponudniki in uvajalci visokotveganih sistemov UI, ki naj bi jih uporabljali javni organi, sprejmejo potrebne ukrepe za izpolnitev zahtev in obveznosti iz te uredbe do ... [šest let od datuma začetka veljavnosti te uredbe].
3. Ponudniki modelov UI za splošne namene, ki so bili dani na trg pred ... [12 mesecev od datuma začetka veljavnosti te uredbe], sprejmejo potrebne ukrepe za izpolnitev obveznosti iz te uredbe do ... [36 mesecev od datuma začetka veljavnosti te uredbe].

Člen 112
Ocena in pregled

1. Komisija enkrat letno po začetku veljavnosti te uredbe in do konca trajanja prenosa pooblastila iz člena 97 oceni potrebo po spremembi seznama iz Priloge III in seznama prepovedanih praks UI iz člena 5. Komisija ugotovitve te ocene predloži Evropskemu parlamentu in Svetu.
2. Komisija do ... [štiri leta od datuma začetka veljavnosti te uredbe] in nato vsaka štiri leta oceni ter Evropskemu parlament in Svetu poroča o naslednjem:
 - (a) potrebi po spremembah za razširitev obstoječih razdelkov področij ali dodajanje novih razdelkov področij v Prilogi III;
 - (b) spremembah seznama sistemov UI, pri katerih so potrebni dodatni ukrepi za preglednost, iz člena 50;
 - (c) spremembah za povečanje učinkovitosti sistema nadzora in upravljanja.

3. Komisija do ... [pet let od datuma začetka veljavnosti te uredbe] ter nato vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe. Poročilo vključuje oceno strukture izvrševanja in morebitno potrebo, da agencija Unije odpravi vse ugotovljene pomanjkljivosti. Temu poročilu na podlagi ugotovitev po potrebi priloži predlog za spremembo te uredbe. Poročila se objavijo.
4. V poročilih iz odstavka 2 se posebna pozornost nameni naslednjemu:
- (a) stanju finančnih, tehničnih in človeških virov pristojnih nacionalnih organov, da se zagotovi učinkovito izvajanje nalog, dodeljenih s to uredbo;
 - (b) stanju kazni, zlasti upravnih glob iz člena 99(1), ki jih države članice uporabljajo za kršitve te uredbe;
 - (c) sprejetim harmoniziranim standardom in skupnim specifikacijam, razvitim v podporo tej uredbi;
 - (d) številu podjetij, ki vstopijo na trg po začetku uporabe te uredbe, in koliko od njih je MSP.

5. Komisija do ... [štiri leta od datuma začetka veljavnosti te uredbe] oceni delovanje Urada za UI, ali je Urad za UI dobil zadostna pooblastila in pristojnosti za izpolnjevanje svojih nalog ter ali bi bilo ustrezno in potrebno za pravilno izvajanje in izvrševanje te uredbe nadgraditi Urad za UI in njegove pristojnosti izvrševanja ter povečati njegove vire. Komisija poročilo o svoji oceni predloži Evropskemu parlamentu in Svetu.
6. Komisija do ... [štiri leta od datuma začetka veljavnosti te uredbe] in nato vsaka štiri leta predloži poročilo o pregledu napredka pri razvoju standardizacijskih dokumentov o energetsko učinkovitem razvoju modelov UI za splošne namene in oceni potrebo po nadaljnjih ukrepih ali dejavnostih, vključno z zavezujočimi ukrepi ali dejavnostmi. Poročilo predloži Evropskemu parlamentu in Svetu ter ga objavi.
7. Komisija do ... [štiri leta od datuma začetka veljavnosti te uredbe] ter nato vsaka tri leta oceni vpliv in učinkovitost prostovoljnih kodeksov ravnanja za spodbujanje uporabe zahtev iz poglavja III, oddelek 2, za sisteme UI, ki niso visokotvegani sistemi UI, in morebitnih drugih dodatnih zahtev za sisteme UI, ki niso visokotvegani sistemi UI, tudi kar zadeva okoljsko trajnostnost.
8. Za namene odstavkov 1 do 7 Odbor, države članice in pristojni nacionalni organi Komisiji na njeno zahtevo in brez nepotrebnega odlašanja zagotovijo informacije.

9. Komisija pri izvajanju ocenjevanj in pregledov iz odstavkov 1 do 7 upošteva stališča in ugotovitve Odbora, Evropskega parlamenta, Sveta ter drugih ustreznih organov ali virov.
10. Komisija po potrebi predloži ustrezne predloge za spremembo te uredbe, zlasti ob upoštevanju razvoja tehnologije, učinkov sistemov UI na zdravje in varnost ter na temeljne pravice in glede na stanje napredka v informacijski družbi.
11. Urad za UI se zaveže, da bo za usmerjanje ocenjevanj in pregledov iz odstavkov 1 do 7 tega člena razvil objektivno in participativno metodologijo za ocenjevanje stopenj tveganja na podlagi meril iz ustreznih členov ter za vključitev novih sistemov na:
 - (a) seznam iz Priloge III, vključno z razširitvijo obstoječih razdelkov področij ali dodajanjem novih razdelkov področij v navedeni prilogi;
 - (b) seznam prepovedanih praks iz člena 5 in
 - (c) seznam sistemov UI, pri katerih so potrebni dodatni ukrepi za preglednost na podlagi člena 50.
12. Pri vsaki spremembi te uredbe na podlagi odstavka 10 ali zadevnih delegiranih ali izvedbenih aktov, ki se nanašajo na sektorsko harmonizacijsko zakonodajo Unije iz oddelka B Priloge I se upoštevajo regulativne posebnosti vsakega sektorja in obstoječi mehanizmi upravljanja, ugotavljanja skladnosti in izvrševanja ter organi, ki so določeni v njih.

13. Komisija do ... [sedem let od datuma začetka veljavnosti te uredbe] oceni izvajanje te uredbe, pri čemer upošteva prva leta njene uporabe, ter o tem poroča Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru. Na podlagi ugotovitev se navedenemu poročilu po potrebi priloži predlog za spremembo te uredbe v zvezi s strukturo izvrševanja in potrebo, da agencija Unije odpravi vse ugotovljene pomanjkljivosti.

Člen 113

Začetek veljavnosti in uporaba

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Uporablja se od ... [24 mesecev od datuma začetka veljavnosti te uredbe].

Vendar se:

- (a) poglavji I in II začneta uporabljati od ... [šest mesecev od datuma začetka veljavnosti te uredbe];
- (b) poglavje III, oddelek 4, poglavje V, poglavje VII in poglavje XII ter člen 78 uporabljajo od ... [12 mesecev od datuma začetka veljavnosti te uredbe], razen člena 101;

- (c) člen 6(1) in ustrezne obveznosti iz te uredbe uporabljajo od ... [36 mesecev od datuma začetka veljavnosti te uredbe].

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament
predsednica

Za Svet
predsednik/predsednica

PRILOGA I

Seznam harmonizacijske zakonodaje Unije

Oddelek A. Seznam harmonizacijske zakonodaje Unije, ki temelji na novem zakonodajnem okviru

1. Direktiva 2006/42/ES Evropskega parlamenta in Sveta z dne 17. maja 2006 o strojih in spremembah Direktive 95/16/ES (UL L 157, 9.6.2006, str. 24);
2. Direktiva 2009/48/ES Evropskega parlamenta in Sveta z dne 18. junija 2009 o varnosti igrač (UL L 170, 30.6.2009, str. 1);
3. Direktiva 2013/53/EU Evropskega parlamenta in Sveta z dne 20. novembra 2013 o plovilih za rekreacijo in osebnih plovilih ter razveljavitvi Direktive 94/25/ES (UL L 354, 28.12.2013, str. 90);
4. Direktiva 2014/33/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaje držav članic v zvezi z dvigali in varnostnimi komponentami za dvigala (UL L 96, 29.3.2014, str. 251);
5. Direktiva 2014/34/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o harmonizaciji zakonodaj držav članic v zvezi z opremo in zaščitnimi sistemi, namenjenimi za uporabo v potencialno eksplozivnih atmosferah (UL L 96, 29.3.2014, str. 309);

6. Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62);
7. Direktiva 2014/68/EU Evropskega parlamenta in Sveta z dne 15. maja 2014 o harmonizaciji zakonodaje držav članic v zvezi z omogočanjem dostopnosti tlačne opreme na trgu (UL L 189, 27.6.2014, str. 164);
8. Uredba (EU) 2016/424 Evropskega parlamenta in Sveta z dne 9. marca 2016 o žičniških napravah in razveljavitvi Direktive 2000/9/ES (UL L 81, 31.3.2016, str. 1);
9. Uredba (EU) 2016/425 Evropskega parlamenta in Sveta z dne 9. marca 2016 o osebni varovalni opremi in razveljavitvi Direktive Sveta 89/686/EGS (UL L 81, 31.3.2016, str. 51);
10. Uredba (EU) 2016/426 Evropskega parlamenta in Sveta z dne 9. marca 2016 o napravah, v katerih zgoreva plinasto gorivo, in razveljavitvi Direktive 2009/142/ES (UL L 81, 31.3.2016, str. 99);
11. Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1);

12. Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o in vitro diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

Oddelek B. Seznam druge harmonizacijske zakonodaje Unije

13. Uredba (ES) št. 300/2008 Evropskega parlamenta in Sveta z dne 11. marca 2008 o skupnih pravilih na področju varovanja civilnega letalstva in o razveljavitvi Uredbe (ES) št. 2320/2002 (UL L 97, 9.4.2008, str. 72);
14. Uredba (EU) št. 168/2013 Evropskega parlamenta in Sveta z dne 15. januarja 2013 o odobritvi in tržnem nadzoru dvo- ali trikolesnih vozil in štirikolesnikov (UL L 60, 2.3.2013, str. 52);
15. Uredba (EU) št. 167/2013 Evropskega parlamenta in Sveta z dne 5. februarja 2013 o odobritvi in tržnem nadzoru kmetijskih in gozdarskih vozil (UL L 60, 2.3.2013, str. 1);
16. Direktiva 2014/90/EU Evropskega parlamenta in Sveta z dne 23. julija 2014 o pomorski opremi in razveljavitvi Direktive Sveta 96/98/ES (UL L 257, 28.8.2014, str. 146);
17. Direktiva (EU) 2016/797 Evropskega parlamenta in Sveta z dne 11. maja 2016 o interoperabilnosti železniškega sistema v Evropski uniji (UL L 138, 26.5.2016, str. 44);

18. Uredba (EU) 2018/858 Evropskega parlamenta in Sveta z dne 30. maja 2018 o odobritvi in tržnem nadzoru motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, spremembi uredb (ES) št. 715/2007 in (ES) št. 595/2009 ter razveljavitvi Direktive 2007/46/ES (UL L 151, 14.6.2018, str. 1);
19. Uredba (EU) 2019/2144 Evropskega parlamenta in Sveta z dne 27. novembra 2019 o zahtevah za homologacijo motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, v zvezi z njihovo splošno varnostjo in zaščito potnikov v vozilu ter izpostavljenih udeležencev v cestnem prometu in o spremembi Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 78/2009, (ES) št. 79/2009 in (ES) št. 661/2009 Evropskega parlamenta in Sveta in uredb Komisije (ES) št. 631/2009, (EU) št. 406/2010, (EU) št. 672/2010, (EU) št. 1003/2010, (EU) št. 1005/2010, (EU) št. 1008/2010, (EU) št. 1009/2010, (EU) št. 19/2011, (EU) št. 109/2011, (EU) št. 458/2011, (EU) št. 65/2012, (EU) št. 130/2012, (EU) št. 347/2012, (EU) št. 351/2012, (EU) št. 1230/2012 in (EU) 2015/166 (UL L 325, 16.12.2019, str. 1);

20. Uredba (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 (UL L 212, 22.8.2018, str. 1), kolikor gre za oblikovanje, proizvodnjo in dajanje na trg zrakoplovov iz člena 2(1), točki (a) in (b), navedene uredbe, kar zadeva brezpilotne zrakoplove in njihove motorje, propelerje, dele in opremo za njihovo daljinsko upravljanje.
-

PRILOGA II

Seznam kaznivih dejanj iz člena 5(1), prvi pododstavek, točka (h)(iii)

Kazniva dejanja iz člena 5(1), prvi pododstavek, točka (h)(iii):

- terorizem,
- trgovina z ljudmi,
- spolno izkoriščanje otrok in otroška pornografija,
- nedovoljena trgovina s prepovedanimi drogami ali psihotropnimi snovmi,
- nedovoljena trgovina z orožjem, strelivom ali eksplozivi,
- umor, huda telesna poškodba,
- nedovoljena trgovina s človeškimi organi ali tkivi,
- nedovoljena trgovina z jedrskimi ali radioaktivnimi snovmi,
- ugrabitev, protipraven odvzem prostosti ali zajetje talcev,
- kazniva dejanja v pristojnosti Mednarodnega kazenskega sodišča,
- nezakonit zaseg zrakoplova ali plovila,

- posilstvo,
 - okoljska kriminaliteta,
 - organiziran ali oborožen rop,
 - sabotaza,
 - sodelovanje v hudodelski združbi, ki je vpletena v eno ali več zgoraj navedenih kaznivih dejanj.
-

PRILOGA III

Visokotvegani sistemi UI iz člena 6(2)

Visokotvegani sistemi UI na podlagi člena 6(2) so sistemi UI, navedeni na seznamu za katero koli od naslednjih področij:

1. biometrika, kolikor je njena uporaba dovoljena na podlagi ustreznega prava Unije ali nacionalnega prava:
 - (a) sistemi za biometrično identifikacijo na daljavo.

To ne vključuje sistemov UI za biometrično preverjanje, katerih edini namen je potrditi, da je določena fizična oseba res ta, za katero se predstavlja;
 - (b) sistemi UI za biometrično kategorizacijo glede na občutljive ali zaščitene lastnosti ali značilnosti na podlagi sklepanja na te lastnosti ali značilnosti;
 - (c) sistemi UI za prepoznavanje čustev;
2. kritična infrastruktura: sistemi UI za uporabo kot varnostne komponente pri upravljanju in delovanju kritične digitalne infrastrukture, cestnega prometa ali pri oskrbi z vodo, plinom, ogrevanjem ali električno energijo;

3. izobraževanje in poklicno usposabljanje:
- (a) sistemi UI za določanje dostopa ali sprejema ali za razvrščanje fizičnih oseb v izobraževalne ustanove in ustanove za poklicno usposabljanje na vseh ravneh;
 - (b) sistemi UI za evalvacijo učnih izidov, tudi kadar se ti izidi uporabljajo za usmerjanje učnega procesa fizičnih oseb v izobraževalnih ustanovah in ustanovah za poklicno usposabljanje na vseh ravneh;
 - (c) sistemi UI za ocenjevanje ustrezne ravni izobrazbe, ki jo bo posameznik prejel ali do katere bo lahko dostopal v okviru ali znotraj izobraževalnih ustanov in ustanov za poklicno usposabljanje na vseh ravneh;
 - (d) sistemi UI za spremljanje in ugotavljanje prepovedanega vedenja učencev in študentov med opravljanjem preizkusov znanja v okviru ali znotraj izobraževalnih ustanov in ustanov za poklicno usposabljanje na vseh ravneh;
4. zaposlovanje, upravljanje delavcev in dostop do samozaposlitve:
- (a) sistemi UI za zaposlovanje ali izbor fizičnih oseb, zlasti za ciljno oglaševanje delovnih mest, analizo in filtriranje prijav za zaposlitev ter ocenjevanje kandidatov;

- (b) sistemi UI za odločanje o pogojih delovnih razmerij, napredovanju ali prenehanju delovnih pogodbenih razmerij, dodeljevanju nalog na podlagi vedenja posameznika oziroma osebnostnih lastnosti ali značilnosti ter spremljanju in ocenjevanju uspešnosti in vedenja oseb v takih razmerjih;

5. uživanje bistvenih zasebnih in javnih storitev in ugodnosti ter dostop do njih:

- (a) sistemi UI, ki naj bi jih uporabljali javni organi ali naj bi se uporabljali v njihovem imenu za ocenjevanje upravičenosti fizičnih oseb do bistvenih ugodnosti in storitev javne pomoči, vključno z zdravstvenimi storitvami, ter za dodelitev, zmanjšanje, preklic ali povračilo takih ugodnosti in storitev;
- (b) sistemi UI za ocenjevanje kreditne sposobnosti fizičnih oseb ali določanje njihove kreditne ocene, razen sistemov UI, ki se uporabljajo za odkrivanje finančnih goljufij;
- (c) sistemi UI za oceno tveganja in oblikovanje cen v zvezi s fizičnimi osebami v primeru življenjskega in zdravstvenega zavarovanja;
- (d) sistemi UI za ocenjevanje in razvrščanje nujnih klicev fizičnih oseb ali za napotitev služb za ukrepanje ob nesrečah, vključno s policijo, gasilci in medicinsko pomočjo, ali določanje prednosti pri njihovi napotitvi, ter sistemi za nujno zdravstveno triažo pacientov;

6. preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, kolikor je njihova uporaba dovoljena na podlagi zadevnega prava Unije ali nacionalnega prava:
- (a) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali v njihovem imenu za oceno tveganja, da fizična oseba postane žrtev kaznivih dejanj;
 - (b) sistemi UI, ki naj bi jih kot poligrafe ali podobna orodja uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj;
 - (c) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za ocenjevanje zanesljivosti dokazov med preiskavo ali pregonom kaznivih dejanj;
 - (d) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za oceno tveganja, ali bi fizična oseba storila ali ponovila kaznivo dejanje, ne samo na podlagi oblikovanja profilov fizičnih oseb iz člena 3(4) Direktive (EU) 2016/680, ali za oceno osebnostnih lastnosti in značilnosti ali preteklega kriminalnega ravnanja fizičnih oseb ali skupin;

- (e) sistemi UI, ki naj bi jih uporabljali organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije v podporo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj za oblikovanje profilov fizičnih oseb iz člena 3(4) Direktive (EU) 2016/680;

7. migracije, azil in upravljanje nadzora meje, kolikor je njihova uporaba dovoljena na podlagi zadevnega prava Unije ali nacionalnega prava:

- (a) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije kot poligrafe ali podobna orodja;
- (b) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije za oceno tveganja, vključno z varnostnim tveganjem, tveganjem nedovoljenih migracij ali zdravstvenim tveganjem, ki ga predstavlja fizična oseba, ki namerava vstopiti ali je vstopila na ozemlje države članice;
- (c) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije za pomoč pristojnim javnim organom pri preučitvi prošenj za azil, vizume in dovoljenja za prebivanje ter s tem povezanih pritožb glede upravičenosti fizičnih oseb, ki so zaprosile za status, vključno s pripadajočimi ocenami zanesljivosti dokazov;

- (d) sistemi UI, ki naj bi jih uporabljali pristojni javni organi ali naj bi se uporabljali v njihovem imenu oziroma naj bi jih uporabljali institucije, organi, uradi in agencije Unije, v okviru migracij, azila in upravljanja nadzora meja za namene odkrivanja, prepoznavanja ali identifikacije fizičnih oseb, z izjemo preverjanja potnih listin;

8. pravosodje in demokratični procesi:

- (a) sistemi UI, ki naj bi jih uporabljal sodni organ ali naj bi se uporabljali v njegovem imenu za pomoč sodnemu organu pri raziskovanju in razlagi dejstev in prava ter pri uporabi prava za konkreten sklop dejstev ali ki naj bi se uporabljali na podoben način pri alternativnem reševanju sporov;
- (b) sistemi UI za vplivanje na izid volitev ali referendumov ali na volilno vedenje fizičnih oseb pri glasovanju na volitvah ali referendumih. To ne vključuje sistemov UI, katerih izhodnim podatkom fizične osebe niso neposredno izpostavljene, kot so orodja, ki se uporabljajo za organizacijo, optimizacijo ali strukturiranje političnih kampanj z upravnega in logističnega vidika.

PRILOGA IV

Tehnična dokumentacija iz člena 11(1)

Tehnična dokumentacija iz člena 11(1) vsebuje vsaj naslednje informacije, kot velja za zadevni sistem UI:

1. splošni opis sistema UI, vključno z:
 - (a) njegovim predvidenim namenom, imenom ponudnika in različico sistema, ki odraža njegovo razmerje do prejšnjih različic;
 - (b) opisom, na kakšen način je sistem UI v interakciji s strojno ali programsko opremo, vključno z drugimi sistemi UI, ki niso del samega sistema UI, ali na kakšen način bi se lahko uporabljal za takšno interakcijo, kadar je ustrezno;
 - (c) različicami ustrezne programske opreme ali strojne programske opreme in morebitnimi zahtevami v zvezi s posodobitvami različice;
 - (d) opisom vseh oblik, v katerih je sistem UI dan na trg ali v uporabo, kot so programski paketi, vgrajeni v strojno opremo, prenosi ali API;
 - (e) opisom strojne opreme, na kateri naj bi sistem UI deloval;
 - (f) kadar je sistem UI sestavni del proizvodov, fotografijami ali ilustracijami, ki prikazujejo zunanje značilnosti, oznake in notranjo razporeditev teh proizvodov;

- (g) osnovnim opisom uporabniškega vmesnika, ki se zagotovi uvajalcu;
- (h) navodili za uvajalca za uporabo in, kadar je ustrezno, osnovnim opisom uporabniškega vmesnika, ki se zagotovi uvajalcu;

2. podroben opis elementov sistema UI in postopka za njegov razvoj, vključno z:

- (a) metodami in ukrepi, izvedenimi za razvoj sistema UI, po potrebi vključno z uporabo prednaučenih sistemov ali orodij, ki so jih zagotovile tretje osebe, in načinom, kako jih je ponudnik uporabil, integriral ali spremenil;
- (b) specifikacijami zasnove sistema, in sicer splošno logiko sistema UI in algoritmov; ključnimi odločitvami glede zasnove sistema, vključno z utemeljitvijo in predpostavkami, tudi glede oseb ali skupin oseb, za katere naj bi se sistem uporabljal; glavnimi izbirami razvrstitve; informacijami o tem, kaj naj bi sistem optimiziral in kako pomembni so različni parametri; opisom pričakovanih izhodnih podatkov sistema in njihovo kakovostjo; odločitvami o morebitnih kompromisih glede tehničnih rešitev, sprejetih za izpolnitev zahtev iz poglavja III, oddelek 2;
- (c) opisom arhitekture sistema, ki pojasnjuje, kako se sestavni deli programske opreme medsebojno nadgrajujejo ali navezujejo in kako so vključeni v celotno obdelavo; računalniškimi viri, uporabljenimi za razvoj, učenje, testiranje in validacijo sistema UI;

- (d) po potrebi zahtevami glede podatkov v zvezi s podatkovnimi listi, ki opisujejo metodologije in tehnike učenja ter uporabljene nabore učnih podatkov, vključno s splošnim opisom teh naborov podatkov, informacijami o njihovem izvoru, obsegu in glavnih značilnostih; načinom, kako so bili podatki pridobljeni in izbrani; postopki označevanja (npr. za nadzorovano učenje), metodologijami čiščenja podatkov (npr. odkrivanje osamelcev);
- (e) oceno potrebnih ukrepov za človeški nadzor v skladu s členom 14, vključno z oceno tehničnih ukrepov, ki jih uvajalci potrebujejo za lažjo razlago izhodnih podatkov sistemov UI, v skladu s členom 13(3), točka (d);
- (f) kadar je ustrezno, podrobnim opisom vnaprej določenih sprememb sistema UI in njegove zmogljivosti skupaj z vsemi ustreznimi informacijami v zvezi s tehničnimi rešitvami, sprejetimi za zagotovitev stalne skladnosti sistema UI z ustreznimi zahtevami iz poglavja III, oddelek 2;
- (g) uporabljenimi postopki validacije in testiranja, vključno z informacijami o uporabljenih validacijskih in testnih podatkih ter njihovih glavnih značilnostih; metrikami, uporabljenimi za merjenje točnosti, robustnosti in skladnosti z drugimi ustreznimi zahtevami iz poglavja III, oddelek 2, pa tudi za merjenje potencialno diskriminatornih vplivov; dnevniki testiranj in vsemi poročili o testiranjih z datumi in podpisi odgovornih oseb, tudi v zvezi z vnaprej določenimi spremembami iz točke (f);
- (h) sprejetimi ukrepi za kibernetško varnost;

3. podrobne informacije o spremljanju, delovanju in nadzoru sistema UI, zlasti glede: njegovih kapacitet in omejitev zmogljivosti, vključno s stopnjami točnosti za določene osebe ali skupine oseb, za katere naj bi se sistem uporabljal, in splošno pričakovano stopnjo točnosti glede na predvideni namen; predvidljivih nenamernih rezultatov in virov tveganj za zdravje in varnost, temeljne pravice in diskriminacijo glede na predvideni namen sistema UI; potrebnih ukrepov za človeški nadzor v skladu s členom 14, vključno s sprejetimi tehničnimi ukrepi, ki uvajalcem omogočajo lažjo razlago izhodnih podatkov sistemov UI; specifikacij o vhodnih podatkih, če je to primerno;
4. opis ustreznosti metrik zmogljivosti za posamezni sistem UI;
5. podroben opis sistema obvladovanja tveganja v skladu s členom 9;
6. opis pomembnih sprememb sistema, ki jih je v njegovem življenjskem ciklu naredil ponudnik;
7. seznam harmoniziranih standardov, ki so bili delno ali v celoti uporabljeni in katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*; kadar taki harmonizirani standardi niso bili uporabljeni, podroben opis rešitev, sprejetih za izpolnitev zahtev iz poglavja III, oddelek 2, vključno s seznamom drugih uporabljenih ustreznih standardov in tehničnih specifikacij;
8. izvod EU izjave o skladnosti iz člena 47;
9. podroben opis vzpostavljenega sistema za ocenjevanje zmogljivosti sistema UI v obdobju po dajanju na trg v skladu s členom 72, vključno z načrtom spremljanja po dajanju na trg iz člena 72(3).

PRILOGA V

EU izjava o skladnosti

EU izjava o skladnosti iz člena 47 vsebuje vse naslednje podatke:

1. ime in vrsto sistema UI ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost sistema UI;
2. ime in naslov ponudnika ali, kadar je ustrezno, njegovega pooblaščenega zastopnika;
3. izjavo, da je za izdajo EU izjave o skladnosti iz člena 47 odgovoren izključno ponudnik;
4. izjavo, da je sistem UI v skladu s to uredbo in po potrebi z drugimi določbami ustreznega prava Unije, ki določa izdajanje EU izjave o skladnosti iz člena 47;
5. kadar sistem UI vključuje obdelavo osebnih podatkov, izjavo, da je sistem UI skladen z uredbama (EU) 2016/679 in (EU) 2018/1725 ter Direktivo (EU) 2016/680;
6. sklice na morebitne uporabljene ustrezne harmonizirane standarde ali druge skupne specifikacije, v zvezi s katerimi je navedena skladnost;

7. kadar je ustrezno, ime in identifikacijsko številko priglšenega organa, opis postopka ugotavljanja skladnosti in identifikacijo izdanega certifikata;
8. kraj in datum izdaje izjave, ime in funkcijo podpisnika ter navedbo, za koga ali v imenu koga ta oseba podpisuje izjavo, in podpis.

PRILOGA VI

Postopek ugotavljanja skladnosti na podlagi notranjega nadzora

1. Postopek ugotavljanja skladnosti na podlagi notranjega nadzora je postopek ugotavljanja skladnosti, ki temelji na točkah 2, 3 in 4.
 2. Ponudnik preveri, ali je vzpostavljeni sistem upravljanja kakovosti usklajen z zahtevami iz člena 17.
 3. Ponudnik preuči informacije iz tehnične dokumentacije, da bi ocenil skladnost sistema UI z ustreznimi bistvenimi zahtevami iz poglavja III, oddelek 2.
 4. Ponudnik tudi preveri, ali sta postopek zasnove in razvoja sistema UI ter njegovo spremljanje po dajanju na trg iz člena 72 skladna s tehnično dokumentacijo.
-

PRILOGA VII

Skladnost na podlagi ocene sistema upravljanja kakovosti in ocene tehnične dokumentacije

1. Uvod

Skladnost na podlagi ocene sistema upravljanja kakovosti in ocene tehnične dokumentacije se ugotovi s postopkom ugotavljanja skladnosti, ki temelji na točkah 2 do 5.

2. Pregled

Odobreni sistem upravljanja kakovosti za načrtovanje, razvoj in testiranje sistemov UI na podlagi člena 17 se preuči v skladu s točko 3 in je predmet nadzora, kot je določeno v točki 5. Tehnična dokumentacija sistema UI se preuči v skladu s točko 4.

3. Sistem upravljanja kakovosti

3.1. Zahtevek ponudnika vključuje:

- (a) ime in naslov ponudnika in, če je zahtevek vložil pooblaščen zastopnik, tudi njegovo ime in naslov;
- (b) seznam sistemov UI, zajetih v istem sistemu upravljanja kakovosti;
- (c) tehnično dokumentacijo za vse sisteme UI, zajete v istem sistemu upravljanja kakovosti;

- (d) dokumentacijo v zvezi s sistemom upravljanja kakovosti, ki zajema vse vidike iz člena 17;
- (e) opis postopkov, ki so vzpostavljeni za ohranjanje ustreznosti in učinkovitosti sistema upravljanja kakovosti;
- (f) pisno izjavo, da isti zahtevek ni bil vložen pri nobenem drugem priglašnem organu.

3.2. Priglašeni organ oceni sistem upravljanja kakovosti, da ugotovi, ali izpolnjuje zahteve iz člena 17.

Odločitev se uradno sporoči ponudniku ali njegovemu pooblaščenemu zastopniku.

Obvestilo vsebuje ugotovitve ocenjevanja sistema upravljanja kakovosti in obrazloženo odločitev o oceni.

3.3. Ponudnik še naprej izvaja in vzdržuje odobreni sistem upravljanja kakovosti, da ostane ustrezen in učinkovit.

3.4. Ponudnik obvesti priglašeni organ o vseh načrtovanih spremembah odobrenega sistema upravljanja kakovosti ali seznama sistemov UI, zajetih v njem.

Priglašeni organ pregleda predlagane spremembe in presodi, ali spremenjeni sistem upravljanja kakovosti še naprej izpolnjuje zahteve iz točke 3.2 oziroma ali je potrebna ponovna ocena.

Priglašeni organ ponudnika uradno obvesti o svoji odločitvi. Obvestilo vsebuje ugotovitve pregleda sprememb in obrazloženo odločitev o oceni.

4. Pregled tehnične dokumentacije

4.1. Ponudnik poleg zahtevka iz točke 3 pri priglašenem organu, ki ga izbere sam, vloži zahtevek za oceno tehnične dokumentacije v zvezi s sistemom UI, ki ga namerava dati na trg ali v uporabo in ki je zajet v sistemu upravljanja kakovosti iz točke 3.

4.2. Zahtevek vključuje:

(a) ime in naslov ponudnika;

(b) pisno izjavo, da enak zahtevek ni bil predložen nobenemu drugemu priglašenemu organu;

(c) tehnično dokumentacijo iz Priloge IV.

4.3. Priglašeni organ pregleda tehnično dokumentacijo. Kadar je primerno in omejeno na to, kar je potrebno za izpolnjevanje njegovih nalog, se priglašenemu organu omogoči neomejen dostop do uporabljenih naborov učnih, validacijskih in testnih podatkov, tudi, kadar je ustrezno in ob uporabi ustreznih varoval, prek API ali z drugimi ustreznimi tehničnimi sredstvi in orodji, ki omogočajo dostop na daljavo.

- 4.4. Pri pregledu tehnične dokumentacije lahko priglašeni organ zahteva, da ponudnik predloži dodatna dokazila ali izvede dodatna testiranja, da se omogoči ustrezna ocena skladnosti sistema UI z zahtevami iz poglavja III, oddelek 2. Kadar priglašeni organ ni zadovoljen s testiranjem, ki jih je opravil ponudnik, neposredno sam opravi ustrezna testiranja, če je to primerno.
- 4.5. Potem ko so bili izkoriščeni in so se izkazali za nezadostne vsi drugi razumni načini preverjanja skladnosti, se priglašenemu organu na obrazloženo zahtevo dovoli tudi dostop do učnih in naučenih modelov sistema UI, vključno z njegovimi relevantnimi parametri, kadar je to potrebno za oceno skladnosti visokotveganega sistema UI z zahtevami iz naslova III, poglavje 2. Za tak dostop se uporablja veljavno pravo Unije in nacionalno pravo o intelektualni lastnini in poslovnih skrivnostih.
- 4.6. Odločitev priglašenega organa se uradno sporoči ponudniku ali njegovemu pooblaščenemu zastopniku. Obvestilo vsebuje ugotovitve ocenjevanja tehnične dokumentacije in obrazloženo odločitev o oceni.

Kadar je sistem UI skladen z zahtevami iz poglavja III, oddelek 2, priglašeni organ izda certifikat Unije o oceni tehnične dokumentacije. V certifikatu so navedeni ime in naslov ponudnika, ugotovitve pregleda, morebitni pogoji za njegovo veljavnost in podatki, potrebni za identifikacijo sistema UI.

V certifikatu in njegovih prilogah so navedene vse potrebne informacije za oceno skladnosti sistema UI in, kadar je ustrezno, nadzor sistema UI med uporabo.

Kadar sistem UI ni skladen z zahtevami iz poglavja III, oddelek 2, priglašeni organ zavrne izdajo certifikata Unije o oceni tehnične dokumentacije ter o tem obvesti vlagatelja in svojo zavrnitev podrobno utemelji.

Kadar sistem UI ne izpolnjuje zahtev glede podatkov, uporabljenih za njegovo učenje, bo pred zahtevkom za novo ugotavljanje skladnosti potrebno ponovno učenje sistema UI. V tem primeru obrazložena odločitev priglašene organa o oceni, s katero zavrne izdajo certifikata Unije o oceni tehnične dokumentacije, vsebuje specifične premisleke glede kakovosti podatkov, uporabljenih za učenje sistema UI, zlasti glede razlogov za neskladnost.

- 4.7. Vsako spremembo sistema UI, ki bi lahko vplivala na njegovo skladnost z zahtevami ali predvidenim namenom, oceni priglašeni organ, ki je izdal certifikat Unije o oceni tehnične dokumentacije. Ponudnik obvesti ta priglašeni organ o svoji nameri, da bo uvedel katero koli od navedenih sprememb, obvesti pa ga tudi, če drugače izve za uvedbo takih sprememb. Priglašeni organ oceni načrtovane spremembe in odloči, ali je zaradi njih potrebno novo ugotavljanje skladnosti v skladu s členom 43(4) oziroma ali bi zadostovala dopolnitev certifikata Unije o oceni tehnične dokumentacije. V slednjem primeru priglašeni organ oceni spremembe, uradno obvesti ponudnika o svoji odločitvi in mu, kadar so spremembe odobrene, izda dopolnilo certifikata Unije o oceni tehnične dokumentacije.

5. Nadzor odobrenega sistema upravljanja kakovosti
- 5.1. Namen nadzora, ki ga izvaja priglašeni organ iz točke 3, je zagotoviti, da ponudnik ustrezno izpolnjuje pogoje odobrenega sistema upravljanja kakovosti.
- 5.2. Za namene ocene ponudnik priglašenemu organu omogoči dostop do prostorov, v katerih potekajo zasnova, razvoj in testiranje sistemov UI. Poleg tega mu posreduje vse potrebne informacije.
- 5.3. Priglašeni organ opravlja redne revizije, s čimer zagotovi, da ponudnik vzdržuje in izvaja sistem upravljanja kakovosti, poročila o teh revizijah pa predloži ponudniku. V okviru teh revizij lahko priglašeni organ izvede dodatna testiranja sistemov UI, za katere je bil izdan certifikat Unije o oceni tehnične dokumentacije.
-

PRILOGA VIII

Informacije, ki se predložijo ob registraciji
visokotveganih sistemov UI v skladu s členom 49

Oddelek A – Informacije, ki jih predložijo ponudniki visokotveganih sistemov UI
v skladu s členom 49(1)

V zvezi z visokotveganimi sistemi UI, ki se registrirajo v skladu s členom 49(1), se predložijo in nato posodablajo naslednje informacije:

1. ime, naslov in kontaktni podatki ponudnika;
2. kadar informacije predloži druga oseba v imenu ponudnika: ime, naslov in kontaktni podatki te osebe;
3. ime, naslov in kontaktni podatki pooblaščenega zastopnika, kadar je ustrezno;
4. trgovsko ime sistema UI ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost sistema UI;
5. opis predvidenega namena sistema UI ter komponent in funkcij, podprtih s tem sistemom UI;
6. kratek in jedrnat opis informacij, ki jih uporablja sistem (podatki, vhodni podatki), in logike delovanja sistema;

7. status sistema UI (na trgu ali v uporabi; ni več na trgu/v uporabi, odpoklican);
8. vrsta, številka in datum izteka veljavnosti certifikata, ki ga je izdal priglašeni organ, ter ime ali identifikacijska številka tega priglašenega organa, kadar je ustrezno;
9. skeniran izvod certifikata iz točke 8, kadar je ustrezno;
10. imena vse držav članic, v katerih je bil sistem UI dan na trg ali v uporabo oziroma je bila omogočena njegova dostopnost v Uniji;
11. izvod EU izjave o skladnosti iz člena 47;
12. elektronska navodila za uporabo; te informacije se ne predložijo za visokotvegane sisteme UI na področjih preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali migracij, azila in upravljanja nadzora meje iz Priloge III, točke 1, 6 in 7;
13. URL za dodatne informacije (neobvezno).

Oddelek B – Informacije, ki jih predložijo ponudniki visokotveganih sistemov UI
v skladu s členom 49(2)

V zvezi z visokotveganimi sistemi UI, ki se registrirajo v skladu s členom 49(2), se predložijo in nato posodablajo naslednje informacije:

1. ime, naslov in kontaktni podatki ponudnika;
2. kadar informacije predloži druga oseba v imenu ponudnika: ime, naslov in kontaktni podatki te osebe;
3. ime, naslov in kontaktni podatki pooblaščenega zastopnika, kadar je ustrezno;
4. trgovsko ime sistema UI ter morebitne dodatne nedvoumne navedbe, ki omogočajo identifikacijo in sledljivost sistema UI;
5. opis predvidenega namena sistema UI;
6. pogoj ali pogoji iz člena 6(3), na podlagi katerih sistem UI ne šteje za visokotvegani;
7. kratek povzetek razlogov, na podlagi katerih sistem UI pri uporabi postopka iz člena 6(3) ne šteje za visokotvegani;
8. status sistema UI (na trgu ali v uporabi; ni več na trgu/v uporabi, odpoklican);
9. imena vseh držav članic, v katerih je bil sistem UI dan na trg ali v uporabo oziroma je bila omogočena njegova dostopnost v Uniji.

Oddelek C – Informacije, ki jih predložijo uvajalci visokotveganih sistemov UI
v skladu s členom 49(3)

V zvezi z visokotveganimi sistemi UI, ki se registrirajo v skladu s členom 49(3), se predložijo in nato posodablajo naslednje informacije:

1. ime, naslov in kontaktni podatki uvajalca;
2. ime, naslov in kontaktni podatki osebe, ki posreduje informacije v imenu uvajalca;
3. URL naslov vnosa sistema UI v podatkovno zbirko EU, za katerega poskrbi njegov ponudnik;
4. povzetek ugotovitev ocene učinka v zvezi s temeljnimi pravicami, ki se opravi v skladu s členom 27;
5. kadar je ustrezno, povzetek ocene učinka v zvezi z varstvom podatkov, izvedene v skladu s členom 35 Uredbe (EU) 2016/679 ali členom 27 Direktive (EU) 2016/680, kot je določeno v členu 26(8) te uredbe.

PRILOGA IX

Informacije, ki se predložijo ob registraciji visokotveganih sistemov UI
v zvezi s testiranjem v realnih razmerah v skladu s členom 60

V zvezi s testiranjem v realnih razmerah, ki se registrira v skladu s členom 60, se predložijo in nato posodablajo naslednje informacije:

1. vseevropska enotna identifikacijska številka testiranja v realnih razmerah;
 2. ime in kontaktni podatki ponudnika ali potencialnega ponudnika in uvajalcev, ki sodelujejo pri testiranju v realnih razmerah;
 3. kratek opis sistema UI, njegov predvideni namen in druge informacije, potrebne za identifikacijo sistema;
 4. povzetek glavnih značilnosti načrta za testiranje v realnih razmerah;
 5. informacije o začasni ali dokončni ustavitvi testiranja v realnih razmerah.
-

PRILOGA X

Zakonodajni akti Unije o obsežnih informacijskih sistemih s področja svobode, varnosti in pravice

1. Schengenski informacijski sistem

- (a) Uredba (EU) 2018/1860 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o uporabi schengenskega informacijskega sistema za vračanje nezakonito prebivajočih državljanov tretjih držav (UL L 312, 7.12.2018, str. 1);
- (b) Uredba (EU) 2018/1861 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju mejnih kontrol, o spremembi Konvencije o izvajanju Schengenskega sporazuma ter o spremembi in razveljavitvi Uredbe (ES) št. 1987/2006 (UL L 312, 7.12.2018, str. 14);
- (c) Uredba (EU) 2018/1862 Evropskega parlamenta in Sveta z dne 28. novembra 2018 o vzpostavitvi, delovanju in uporabi schengenskega informacijskega sistema (SIS) na področju policijskega sodelovanja in pravosodnega sodelovanja v kazenskih zadevah, o spremembi in razveljavitvi Sklepa Sveta 2007/533/PNZ ter o razveljavitvi Uredbe (ES) št. 1986/2006 Evropskega parlamenta in Sveta in Sklepa Komisije 2010/261/EU (UL L 312, 7.12.2018, str. 56).

2. Vizumski informacijski sistem

- (a) Uredba (EU) 2021/1133 Evropskega parlamenta in Sveta z dne 7. julija 2021 o spremembi uredb (EU) št. 603/2013, (EU) 2016/794, (EU) 2018/1862, (EU) 2019/816 in (EU) 2019/818 v zvezi z določitvijo pogojev za dostop do drugih informacijskih sistemov EU za namene Vizumskega informacijskega sistema (UL L 248, 13.7.2021, str. 1).
- (b) Uredba (EU) 2021/1134 Evropskega parlamenta in Sveta z dne 7. julija 2021 o spremembi uredb (ES) št. 767/2008, (ES) št. 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 in (EU) 2019/1896 Evropskega parlamenta in Sveta ter razveljavitvi Odločbe Sveta 2004/512/ES in Sklepa Sveta 2008/633/PNZ zaradi reforme Vizumskega informacijskega sistema (UL L 248, 13.7.2021, str. 11).

3. Eurodac

Uredba (EU) 2024/... Evropskega parlamenta in Sveta o vzpostavitvi sistema Eurodac za primerjavo biometričnih podatkov zaradi učinkovite uporabe Uredbe (EU) 2024/... [uredba o upravljanju azila in migracij], Uredbe (EU) 2024/... [uredba o preselitvi] in Direktive 2001/55/ES [Direktiva o začasni zaščiti] za ugotavljanje istovetnosti nezakonito prebivajočih državljanov tretjih držav ali oseb brez državljanstva ter o zahtevah za primerjavo s podatki iz sistema Eurodac, ki jih vložijo organi kazenskega pregona držav članic in Europol za namene kazenskega pregona, ter o spremembi uredb (EU) 2018/1240 in (EU) 2019/818⁺.

4. Sistem vstopa/izstopa

Uredba (EU) 2017/2226 Evropskega parlamenta in Sveta z dne 30. novembra 2017 o vzpostavitvi sistema vstopa/izstopa (SVI) za evidentiranje podatkov o vstopu in izstopu ter podatkov o zavrnitvi vstopa državljanov tretjih držav pri prehajanju zunanjih meja držav članic in določitvi pogojev za dostop do SVI zaradi preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter o spremembi Konvencije o izvajanju Schengenskega sporazuma in uredb (ES) št. 767/2008 ter (EU) št. 1077/2011 (UL L 327, 9.12.2017, str. 20).

⁺ UL: prosimo, da v besedilo vstavite številko uredbe iz dokumenta PE-CONS 15/24 (2016/0132(COD)) ter v opombo vstavite številko, datum, naslov in sklic na UL za navedeno uredbo.

5. Evropski sistem za potovalne informacije in odobritve
- (a) Uredba (EU) 2018/1240 Evropskega parlamenta in Sveta z dne 12. septembra 2018 o vzpostavitvi Evropskega sistema za potovalne informacije in odobritve (ETIAS) ter spremembi uredb (EU) št. 1077/2011, (EU) št. 515/2014, (EU) 2016/399, (EU) 2016/1624 in (EU) 2017/2226 (UL L 236, 19.9.2018, str. 1);
 - (b) Uredba (EU) 2018/1241 Evropskega parlamenta in Sveta z dne 12. septembra 2018 o spremembi Uredbe (EU) 2016/794 za namene vzpostavitve Evropskega sistema za potovalne informacije in odobritve (ETIAS) (UL L 236, 19.9.2018, str. 72).

6. Evropski informacijski sistem kazenskih evidenc za državljane tretjih držav in osebe brez državljanstva

Uredba (EU) 2019/816 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o vzpostavitvi centraliziranega sistema za določitev držav članic, ki imajo informacije o obsodbah državljanov tretjih držav in oseb brez državljanstva (sistem ECRIS-TCN), z namenom dopolnitve evropskega informacijskega sistema kazenskih evidenc ter o spremembi Uredbe (EU) 2018/1726 (UL L 135, 22.5.2019, str. 1).

7. Interoperabilnost

- (a) Uredba (EU) 2019/817 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju meja in vizumov ter spremembi uredb (ES) št. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 in (EU) 2018/1861 Evropskega parlamenta in Sveta ter Odločbe Sveta 2004/512/ES in Sklepa Sveta 2008/633/PNZ (UL L 135, 22.5.2019, str. 27);
 - (b) Uredba (EU) 2019/818 Evropskega parlamenta in Sveta z dne 20. maja 2019 o vzpostavitvi okvira za interoperabilnost informacijskih sistemov EU na področju policijskega in pravosodnega sodelovanja, azila ter migracij in spremembi uredb (EU) 2018/1726, (EU) 2018/1862 ter (EU) 2019/816 (UL L 135, 22.5.2019, str. 85).
-

PRILOGA XI

Tehnična dokumentacija iz člena 53(1), točka (a) – tehnična dokumentacija
za ponudnike modelov UI za splošne namene

Oddelek 1

Informacije, ki jih predložijo vsi ponudniki modelov UI za splošne namene

Tehnična dokumentacija iz člena 53(1), točka (a), vsebuje vsaj naslednje informacije, odvisno od velikosti in profila tveganja modela:

1. splošni opis modela UI za splošne namene, vključno z:
 - (a) nalogami, ki naj bi jih model opravljal, ter vrsto in naravo sistemov UI, v katere se lahko vključi;
 - (b) veljavnimi politikami glede sprejemljive uporabe;
 - (c) datumom, na katerega je bil objavljen, in metodami distribucije;
 - (d) arhitekturo in številom parametrov;
 - (e) načinom (npr. besedilo, slika) ter obliko vhodnih in izhodnih podatkov;
 - (f) licenco;

2. podrobni opis elementov modela iz točke 1 in ustrezne informacije o postopku razvoja, vključno z naslednjimi elementi:
- (a) tehničnimi sredstvi (npr. navodila za uporabo, infrastruktura, orodja), potrebnimi za vključitev modela UI za splošne namene v sisteme UI;
 - (b) specifikacijami zasnove modela in postopkom učenja, vključno z metodologijami in tehnikami učenja, ključnimi odločitvami glede zasnove, tudi utemeljitev in predpostavke; informacijami o tem, kaj naj bi model optimiziral in kako pomembni so različni parametri, kot je ustrezno;
 - (c) informacijami o podatkih, uporabljenih za učenje, testiranje in validacijo, kadar je primerno, vključno z vrsto in izvorom podatkov ter metodologijami urejanja (npr. čiščenje, filtriranje itd.), številom podatkovnih točk, njihovim obsegom in glavnimi značilnostmi; načinom pridobitve in izbire podatkov ter po potrebi vsemi drugimi ukrepi za odkrivanje neprimernosti virov podatkov in metod za zaznavanje prepoznavnih pristranskosti;
 - (d) računalniškimi viri, ki se uporabljajo za učenje modela (npr. število operacij s plavajočo vejico), čas učenja in druge pomembne podrobnosti v zvezi z učenjem;
 - (e) znano ali ocenjeno energetska poraba modela.

Kadar energetska poraba modela iz točke (e) ni znana, lahko energetska poraba temelji na informacijah o uporabljenih računalniških virih.

Oddelek 2

Dodatne informacije, ki jih predložijo
ponudniki modelov UI za splošne namene s sistemskim tveganjem

1. podrobni opis strategij ocenjevanja, vključno z rezultati ocenjevanja, na podlagi razpoložljivih javnih protokolov in orodij za ocenjevanje ali drugih metodologij za ocenjevanje. Strategije ocenjevanja vključujejo merila za ocenjevanje, metrike in metodologijo za opredelitev omejitev;
 2. kadar je ustrezno, podrobni opis ukrepov, sprejetih za izvajanje notranjega in/ali zunanjega preskušanja po načelu kontradiktornosti (npr. etični heking) in prilagoditve modela, vključno z uskladitvami in izpopolnitvami;
 3. kadar je ustrezno, podrobni opis arhitekture sistema, ki pojasnjuje, kako se sestavni deli programske opreme medsebojno nadgrajujejo ali navezujejo in kako so vključeni v celotno obdelavo.
-

PRILOGA XII

Informacije o preglednosti iz člena 53(1), točka (b)

– tehnična dokumentacija, ki jo ponudniki modelov UI za splošne namene dajo na razpolago ponudnikom nižje v verigi, ki model vključijo v svoj sistem UI

Informacije iz člena 53(1), točka (b), vsebujejo vsaj naslednje:

1. splošni opis modela UI za splošne namene, vključno z:
 - (a) nalogami, ki naj bi jih model opravljal, ter vrsto in naravo sistemov UI, v katere se lahko vključi;
 - (b) veljavnimi politikami glede sprejemljive uporabe;
 - (c) datumom, na katerega je bil objavljen, in metodami distribucije;
 - (d) opisom, na kakšen način je model v interakciji s strojno ali programsko opremo, ki ni del samega modela, ali na kakšen način bi se lahko uporabljal za takšno interakcijo, kadar je ustrezno;
 - (e) različicami ustrezne programske opreme, povezane z uporabo modela UI za splošne namene, kadar je to ustrezno;
 - (f) arhitekturo in številom parametrov;
 - (g) načinom (npr. besedilo, slika) ter obliko vhodnih in izhodnih podatkov;
 - (h) licenco za model;

2. opis elementov modela in postopka za njegov razvoj, vključno s:
- (a) tehničnimi sredstvi (npr. navodila za uporabo, infrastruktura, orodja), potrebnimi za vključitev modela UI za splošne namene v sisteme UI;
 - (b) načinom (npr. besedilo, slika itd.) ter obliko vhodnih in izhodnih podatkov, pa tudi njihovo največjo velikostjo (npr. dolžina vsebinskega okna itd.);
 - (c) informacijami o podatkih, uporabljenih za učenje, testiranje in validacijo, kadar je primerno, vključno z vrsto in izvorom podatkov ter metodologijami urejanja.
-

PRILOGA XIII

Merila za označitev modelov UI za splošne namene s sistemskim tveganjem iz člena 51

Pri ugotavljanju, ali ima model UI za splošne namene zmogljivosti ali vpliv, enakovredne tistim iz člena 51(1), točka (a), Komisija upošteva naslednja merila:

- (a) število parametrov modela;
- (b) kakovost ali velikost nabora podatkov, merjeno na primer z žetoni;
- (c) količino izračuna, uporabljeno za učenje modela, merjeno z operacijami s plavajočo vejico ali izraženo s kombinacijo drugih spremenljivk, kot so ocenjeni stroški učenja, predvideni čas, potreben za učenje, ali ocenjena poraba energije za učenje;
- (d) vhodne in izhodne načine modela, kot so besedilo v besedilo (veliki jezikovni modeli), besedilo v podobo, večmodalnost in najsodobnejši pragovi za določanje zmogljivosti z visoko učinkovitostjo za vsak način, ter posebna vrsta vhodnih in izhodnih podatkov (npr. biološka zaporedja);
- (e) merila uspešnosti in ocenjevanja zmogljivosti modela, vključno z upoštevanjem števila nalog brez dodatnega učenja, prilagodljivostjo za učenje novih, različnih nalog, njegovo stopnjo avtonomije in nadgradljivosti ter orodji, do katerih ima dostop;

- (f) ali ima velik vpliv na notranji trg zaradi svojega dosega, na katerega se domneva, ko je bil dan na voljo vsaj 10 000 registriranim poslovnim uporabnikom s sedežem v Uniji;
 - (g) število registriranih končnih uporabnikov.“
-