Conseil de
l'Union européenne

Bruxelles, le 22 janvier 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2024) 7 final
Objet:	RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL sur le premier réexamen du fonctionnement des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE

Les délégations trouveront ci-joint le document COM(2024) 7 final.

p.j.: COM(2024) 7 final

COMMISSION
EUROPÉENNE

Bruxelles, le 15.1.2024
COM(2024) 7 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

sur le premier réexamen du fonctionnement des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE

{SWD(2024) 3 final}

1. LE PREMIER RÉEXAMEN – HISTORIQUE ET CONTEXTE

Le présent rapport présente les conclusions de la Commission concernant le premier réexamen des décisions d'adéquation adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE[1] (ci-après la «directive sur la protection des données»).

Dans ces décisions, la Commission a constaté que onze pays ou territoires assurent un niveau de protection adéquat des données à caractère personnel transférées depuis l'Union européenne (ci-après l'«UE»)[2], à savoir l'Andorre[3], l'Argentine[4], le Canada (pour les opérateurs commerciaux)[5], les Îles Féroé[6], Guernesey[7], l'Île de Man[8], Israël[9], Jersey[10], la Nouvelle-Zélande[11], la Suisse[12] et l'Uruguay[13]. En conséquence, les transferts de données de l'UE vers ces pays ou territoires peuvent avoir lieu sans exigences supplémentaires.

[1] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

[2] À la suite de son intégration dans l'accord sur l'Espace économique européen (ci-après l'«accord EEE»), le RGPD s'applique également à la Norvège, à l'Islande et au Liechtenstein. Toute référence à l'UE dans le présent rapport doit être comprise comme incluant également les États de l'EEE.

[3] Décision 2010/625/UE de la Commission du 19 octobre 2010 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré en Andorre (JO L 277 du 21.10.2010, p. 27).

[4] Décision 2003/490/CE de la Commission du 30 juin 2003 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'Argentine (JO L 168 du 5.7.2003, p. 19).

[5] Décision 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques (JO L 2 du 4.1.2002, p. 13).

[6] Décision 2010/146/UE de la Commission du 5 mars 2010 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat assuré par la loi des Îles Féroé relative au traitement des données à caractère personnel (JO L 58 du 9.3.2010, p. 17).

[7] Décision 2003/821/CE de la Commission du 21 novembre 2003 constatant le niveau de protection adéquat des données à caractère personnel à Guernesey (JO L 308 du 25.11.2003, p. 27).

[8] Décision 2004/411/CE de la Commission du 28 avril 2004 constatant le niveau de protection adéquat des données à caractère personnel dans l'Île de Man (JO L 151 du 30.4.2004, p. 48).

[9] Décision 2011/61/UE de la Commission du 31 janvier 2011 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'État d'Israël concernant le traitement automatisé des données à caractère personnel (JO L 27 du 1.2.2011, p. 39).

[10] Décision 2008/393/CE de la Commission du 8 mai 2008 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré à Jersey (JO L 138 du 28.5.2008, p. 21).

[11] Décision d'exécution 2013/65/UE de la Commission du 19 décembre 2012 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Nouvelle-Zélande (JO L 28 du 30.1.2013, p. 12).

[12] Décision 2000/518/CE de la Commission du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse (JO L 215 du 25.8.2000, p. 1).

[13] Décision d'exécution 2012/484/UE de la Commission du 21 août 2012 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la République orientale de l'Uruguay concernant le traitement automatisé des données à caractère personnel (JO L 227 du 23.8.2012, p. 11).

Après l'entrée en application du règlement (UE) 2016/679[14] (ci-après le «RGPD») le 25 mai 2018, les décisions d'adéquation adoptées en vertu de la directive sur la protection des données sont restées en vigueur[15]. Dans le même temps, le RGPD a précisé que les constats d'adéquation constituent des «instruments vivants», en disposant que la Commission doit suivre, de manière permanente, les évolutions dans les pays tiers qui pourraient porter atteinte au fonctionnement des décisions d'adéquation existantes[16]. En outre, l'article 97 du RGPD impose à la Commission de réexaminer périodiquement ces décisions (tous les quatre ans), afin de déterminer si les pays et les territoires ayant bénéficié d'un constat d'adéquation continuent d'assurer un niveau de protection adéquat des données à caractère personnel.

Le premier réexamen des décisions d'adéquation adoptées en vertu de l'ancien cadre de protection des données de l'UE a été entrepris dans le cadre d'une évaluation plus générale de l'application et du fonctionnement du RGPD, à l'issue de laquelle la Commission a présenté ses conclusions dans sa communication intitulée «La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique – deux années d'application du règlement général sur la protection des données»[17]. Toutefois, la conclusion portant sur cet aspect du réexamen a été différée afin de tenir compte de l'arrêt de la Cour de justice dans l'affaire *Schrems II*[18], dans lequel la Cour a apporté des précisions importantes sur certains éléments clés de la norme dite de «l'adéquation», ainsi que sur d'autres évolutions connexes. Cela a donné lieu à des échanges approfondis avec les pays et les territoires concernés sur divers aspects de leur cadre juridique, de leurs mécanismes de surveillance et de leur système d'application des règles[19]. Le présent rapport tient pleinement compte de l'ensemble de ces évolutions, tant dans l'UE que dans les pays tiers et les territoires concernés.

Il est important de noter que ce premier réexamen a lieu dans un contexte de développement exponentiel des technologies numériques. Au cours des dernières décennies, l'importance des décisions d'adéquation s'est considérablement accrue, car les flux de données sont devenus une composante incontournable de la transformation numérique de la société et de la mondialisation

[14] 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).

[15] Voir article 45, paragraphe 9, du RGPD, qui dispose que les décisions adoptées par la Commission sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission adoptée conformément au paragraphe 3 ou 5 de l'article 45.

[16] Article 45, paragraphe 4, du RGPD. Voir également arrêt de la Cour de justice du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner (*Schrems I*), EU:C:2015:650, point 76.

[17] La communication a été publiée en juin 2020 et est disponible à l'adresse suivante: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_fr.

[18] Voir également arrêt de la Cour de justice du 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner/Facebook Ireland Ltd et Maximillian Schrems (*Schrems II*), EU:C:2020:559.

[19] La décision d'adéquation concernant le Japon a été adoptée sur la base du RGPD et prévoit un examen périodique distinct. Le premier examen s'est achevé en avril 2023 par la publication du rapport de la Commission au Parlement européen et au Conseil sur le premier examen du fonctionnement de la décision d'adéquation pour le Japon [COM(2023) 275 final], disponible à l'adresse suivante: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=COM:2023:275:FIN

de l'économie. Le transfert transfrontière de données fait désormais partie intégrante des opérations quotidiennes des entreprises européennes de toutes tailles et de tous secteurs. Plus que jamais, le respect de la vie privée est une condition nécessaire à la stabilité, à la sécurité et à la compétitivité des flux commerciaux. Dans ce contexte, les décisions d'adéquation jouent un rôle de plus en plus important, à bien des égards. En permettant que, lorsque des données sont transférées, elles continuent de bénéficier de la protection, ces décisions favorisent des flux de données sûrs et respectueux des droits individuels, conformément à l'approche de l'UE en matière de transformation numérique, centrée sur l'humain. En reconnaissant que le cadre de protection de la vie privée d'un pays tiers offre un niveau de protection substantiellement équivalent à celui de l'UE, elles favorisent la convergence des systèmes de protection de la vie privée fondés sur des normes de protection élevées. En outre, comme il est expliqué dans le présent rapport, plutôt que de constituer une «fin en soi», les décisions d'adéquation ont posé les bases d'une coopération plus étroite et d'une convergence réglementaire plus poussée entre l'UE et des partenaires animés du même esprit. En permettant la libre circulation des données à caractère personnel, ces décisions ont ouvert des canaux commerciaux pour les opérateurs de l'UE, notamment en complétant et en amplifiant les avantages des accords commerciaux, ainsi qu'en facilitant la coopération avec des partenaires étrangers dans un grand nombre de domaines réglementaires. En offrant une solution simple et complète aux transferts de données, sans que l'exportateur des données ait besoin de fournir des garanties supplémentaires ou d'obtenir une autorisation, elles facilitent le respect des exigences du RGPD en matière de transfert international, en particulier pour les petites et les moyennes entreprises. Enfin, grâce à leur «effet de réseau», les décisions d'adéquation adoptées par la Commission européenne revêtent une importance croissante, même en dehors de l'UE, car elles permettent non seulement la libre circulation des données avec les 30 économies de l'UE, mais aussi avec de nombreux autres pays ou territoires dans le monde[20], qui reconnaissent les pays pour lesquels il existe une décision d'adéquation de l'UE comme des «destinations sûres» selon leurs propres règles de protection des données.

Pour toutes ces raisons, comme le confirme également le dialogue intense et fructueux engagé avec les pays/territoires tiers concernés qui sous-tend le présent réexamen, les décisions d'adéquation sont devenues une composante stratégique de la relation globale de l'UE avec ces partenaires étrangers et sont reconnues comme un outil essentiel pour l'approfondissement des relations de coopération dans un grand nombre de domaines. Il est donc particulièrement important que ces décisions puissent résister à l'épreuve du temps et faire face à de nouveaux développements et défis.

2. OBJET ET MÉTHODOLOGIE DU RÉEXAMEN

Les décisions d'adéquation qui font l'objet du présent réexamen ont été adoptées au titre du cadre de protection des données de l'UE ayant précédé le RGPD. Si les décisions les plus récentes remontent à une dizaine d'années (par exemple, les décisions relatives à la Nouvelle-Zélande et à l'Uruguay, toutes deux adoptées en 2012), d'autres sont en vigueur depuis plus de vingt ans (par exemple, celles relatives au Canada, adoptée en 2001, et à la Suisse, adoptée en

[20] Par exemple, l'Argentine, la Colombie, Israël, le Maroc, la Suisse et l'Uruguay.

2000). Depuis, les cadres de protection des données des onze pays et territoires ont évolué, par exemple du fait de réformes législatives ou réglementaires, de l'évolution des pratiques d'application des règles des autorités chargées de la protection des données ou de l'évolution de la jurisprudence.

Lors de son évaluation, la Commission s'est donc concentrée sur l'évolution des cadres de protection des données des pays et des territoires concernés depuis l'adoption de la décision d'adéquation. Elle s'est attachée à déterminer dans quelle mesure ces évolutions ont continué de façonner le paysage de la protection des données du pays ou du territoire concerné et si, compte tenu de ces évolutions, les différents régimes continuent d'assurer un niveau de protection adéquat.

À cette fin, l'évolution du régime de protection des données de l'UE, notamment l'entrée en vigueur du RGPD, a été pleinement prise en considération. En particulier, depuis l'adoption de ces décisions d'adéquation, la norme juridique applicable à ces décisions ainsi que les éléments dont il faut tenir compte pour déterminer si un système étranger assure un niveau de protection adéquat ont été précisés par la jurisprudence de la Cour de justice et par les lignes directrices adoptées par le groupe de travail «Article 29» et son successeur, le comité européen de la protection des données[21] (ci-après l'«EDPB»).

La Cour de justice, dans son arrêt du 6 octobre 2015 dans l'affaire *Schrems I,* a notamment établi que, s'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'UE, le principe de l'adéquation doit être compris comme exigeant un niveau de protection «substantiellement équivalent»[22]. En particulier, la Cour a précisé que les moyens auxquels ce pays tiers a recours aux fins de la protection des données à caractère personnel peuvent être différents de ceux mis en œuvre au sein de l'Union, pour autant qu'ils s'avèrent, en pratique, effectifs afin d'assurer un niveau de protection adéquat[23]. Le principe de l'adéquation exige donc une analyse approfondie du système du pays tiers dans son ensemble, notamment la substance de ses mesures de protection de la vie privée, leur mise en œuvre effective et le contrôle de leur application.

En outre, la Cour a précisé que l'évaluation de la Commission ne doit pas se limiter au cadre général régissant la protection des données dans le pays tiers concerné, mais doit également inclure les règles régissant l'accès des autorités publiques aux données à caractère personnel, en particulier pour des raisons de respect de la loi et de sécurité nationale[24]. En invoquant la charte des droits fondamentaux, la Cour a recensé plusieurs exigences auxquelles ces règles doivent répondre pour satisfaire à la norme dite de l'«équivalence substantielle». Par exemple, la législation en vigueur dans ce domaine doit prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties

[21] Le comité européen de la protection des données réunit les autorités de contrôle de la protection des données des États membres et le Contrôleur européen de la protection des données.
[22] Arrêt *Schrems I*, points 73, 74 et 96. Voir également considérant 104 du règlement (UE) 2016/679, qui fait référence à la norme dite de l'«équivalence essentielle».
[23] Arrêt *Schrems I*, point 74.
[24] Arrêt *Schrems I*, point 90.

suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données[25]. Elle doit également prévoir la possibilité pour les justiciables d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données[26].

Le RGPD s'est appuyé sur les précisions apportées par la Cour de justice pour répertorier de manière détaillée les éléments que la Commission doit prendre en considération lors d'une évaluation de l'adéquation[27]. Par ailleurs, dans l'arrêt *Schrems II* du 16 juillet 2020, la Cour de justice s'est davantage attardée sur la norme dite de l'«équivalence substantielle», notamment en ce qui concerne les règles régissant l'accès des autorités publiques aux données à caractère personnel à des fins de respect de la loi et de sécurité nationale. En particulier, elle y a précisé que la norme dite de l'«équivalence substantielle» exige que les cadres juridiques revêtant un caractère contraignant pour les autorités publiques des pays et des territoires tiers concernés comprennent des exigences minimales garantissant que ces autorités ne peuvent pas accéder aux données au-delà de ce qui est nécessaire et proportionné aux objectifs légitimes poursuivis, et que les personnes concernées jouissent de droits effectifs et opposables à ces autorités[28].

L'évolution de la norme dite de «l'adéquation» se reflète également dans les lignes directrices initialement adoptées par le groupe de travail «Article 29», et ultérieurement entérinées par l'EDPB[29]. Ces lignes directrices, et en particulier les «critères de référence pour l'adéquation», précisent plus avant les éléments que la Commission doit prendre en considération lors de la réalisation d'une évaluation d'adéquation, notamment en fournissant une vue d'ensemble des «garanties essentielles» pour l'accès des autorités publiques aux données à caractère personnel. Elles s'appuient notamment sur la jurisprudence de la Cour européenne des droits de l'homme et ont été mises à jour par l'EDPB pour tenir compte des précisions apportées par la Cour de justice dans l'arrêt *Schrems II*[30]. Il est important de noter que les critères de référence pour l'adéquation reconnaissent également que la norme dite de l'«équivalence substantielle» ne nécessite pas de reproduction point par point («photocopie») des règles de l'UE, étant donné que les moyens d'assurer un niveau de protection comparable peuvent varier d'un système de protection à l'autre et reflètent souvent des traditions juridiques différentes.

Par conséquent, pour déterminer si les onze décisions d'adéquation adoptées au titre des anciennes règles continuent de répondre à la norme fixée par le RGPD, la Commission a non seulement tenu compte de l'évolution des cadres de protection des données dans les pays et les territoires concernés, mais également de l'évolution de l'interprétation de la norme dite de l'«adéquation» elle-même, selon le droit de l'UE. L'évaluation porte également sur le cadre

[25]Arrêt *Schrems I*, point 91.
[26]Arrêt *Schrems I*, point 95.
[27] Article 45, paragraphe 2, du RGPD.
[28]Arrêt *Schrems II*, points 180 à 182.
[29] Critères de référence pour l'adéquation, WP 254 rev. 01, 6 février 2018 (document disponible à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30]Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance (document disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_fr).

juridique régissant l'accès aux données à caractère personnel transférées depuis l'UE et l'utilisation desdites données par les autorités publiques des pays ou des territoires offrant un niveau de protection adéquat sur la base de l'article 25, paragraphe 6, de la directive sur la protection des données.

3. RÉEXAMEN

Comme exposé ci-dessus, pour chacun des pays ou territoires concernés, l'évaluation des décisions d'adéquation existantes porte sur le cadre de protection des données et sur toute évolution de ce cadre juridique depuis l'adoption de la décision d'adéquation, ainsi que sur les règles régissant l'accès des pouvoirs publics aux données – notamment pour des raisons de respect de la loi et de sécurité nationale. Au cours de ces dernières années, les services de la Commission ont pris plusieurs mesures pour procéder à cette évaluation, en étroite collaboration avec chacun des pays ou des territoires concernés.

Afin d'aider la Commission à s'acquitter de ses obligations de surveillance, chacun des onze pays ou territoires a fourni à la Commission des informations complètes sur l'évolution de son régime de protection des données depuis l'adoption de la décision d'adéquation. En outre, la Commission a demandé à chacun des onze pays ou territoires des informations détaillées sur les règles régissant, dans sa juridiction, l'accès des autorités publiques aux données à caractère personnel, en particulier à des fins de respect de la loi et de sécurité nationale. La Commission a également sollicité des informations auprès de sources publiques, d'autorités de surveillance et d'autorités chargées de faire appliquer la législation, ainsi que d'experts locaux sur le fonctionnement des décisions et sur les évolutions pertinentes de la loi et de la pratique de chacun des pays et des territoires concernés, tant en ce qui concerne les règles de protection des données applicables aux opérateurs privés qu'en ce qui concerne l'accès des pouvoirs publics. Enfin, le cas échéant, il a été dûment tenu compte des engagements internationaux souscrits par ces pays ou territoires au titre d'instruments régionaux ou universels.

Sur cette base, la Commission a entamé un dialogue intense avec chacun des pays et des territoires concernés. Dans le cadre de ce dialogue, la plupart de ces pays et territoires ont modernisé et renforcé leur législation en matière de protection de la vie privée au moyen de réformes globales ou partielles (par exemple, l'Andorre, le Canada, les Îles Féroé, la Suisse, la Nouvelle-Zélande), motivées entre autres par la nécessité d'assurer la continuité des décisions d'adéquation. Certains de ces pays ont adopté des réglementations et/ou les lignes directrices émises par leur autorité de protection des données en vue d'introduire de nouvelles exigences en matière de protection des données (par exemple, Israël, l'Uruguay) ou de clarifier certaines règles en matière de vie privée (par exemple, l'Argentine, le Canada, Guernesey, Jersey, l'Île de Man, Israël, la Nouvelle-Zélande), en s'appuyant sur les pratiques en matière d'application de la législation ou la jurisprudence. En outre, afin de remédier aux différences importantes de niveau de protection, des garanties supplémentaires concernant les données à caractère personnel transférées depuis l'Europe ont été négociées et convenues avec certains des pays et des territoires concernés, lorsque cela était nécessaire pour assurer la continuité de la décision d'adéquation. À titre d'exemple, le gouvernement canadien a étendu les droits d'accès et de rectification des données à caractère personnel traitées par le secteur public à tout individu,

quelle que soit sa nationalité ou son lieu de résidence (alors que ces droits n'étaient auparavant accessibles qu'aux citoyens canadiens, aux résidents permanents ou aux personnes présentes au Canada)[31]. Autre exemple, le gouvernement israélien a mis en place des garanties spécifiques pour renforcer la protection des données à caractère personnel transférées depuis l'Espace économique européen, qui créent notamment de nouvelles obligations dans le domaine de l'exactitude et de la conservation des données, renforcent les droits à l'information et à l'effacement et introduisent de nouvelles catégories de données sensibles[32].

Parallèlement, les services de la Commission ont recueilli les points de vue du Parlement européen (commission des libertés civiles, de la justice et des affaires intérieures)[33], du Conseil (par l'entremise du groupe de travail sur la protection des données)[34], de l'EDPB[35] et du groupe d'experts multipartite du RGPD[36] (composé de représentants de la société civile et de l'industrie, d'universitaires et de praticiens du droit) et les ont régulièrement tenus informés de l'état d'avancement de l'évaluation.

Le présent rapport et le document de travail des services de la Commission qui l'accompagne sont donc le fruit d'une collaboration étroite avec chacun des pays et des territoires concernés, ainsi que d'une consultation avec les institutions et les organes compétents de l'UE et de contributions de leur part. Ils s'appuient sur diverses sources, notamment la législation, les actes réglementaires, la jurisprudence, les décisions et les orientations des autorités de protection des données, les rapports d'organismes de surveillance (indépendants) et les contributions des parties prenantes. Avant l'adoption du présent rapport, tous les pays et les territoires susmentionnés ont eu la possibilité de vérifier l'exactitude factuelle des informations fournies dans le document de travail des services de la Commission concernant leur système.

4. PRINCIPALES CONSTATATIONS ET CONCLUSIONS

Le premier réexamen a démontré que, depuis l'adoption des décisions d'adéquation, les cadres de protection des données en vigueur dans chacun des onze pays ou territoires ont convergé davantage vers le cadre de l'UE. En outre, en matière d'accès des pouvoirs publics aux données à caractère personnel, il a montré que la législation de ces pays ou territoires impose des

[31] Article 12 de la Loi sur la protection des renseignements personnels, décret d'extension nº 1 de la loi sur la protection des renseignements personnels et décret d'extension nº 2 de la loi sur la protection des renseignements personnels.

[32] Règlement sur la protection de la vie privée (instructions pour les données transférées en Israël depuis l'Espace économique européen), 5783-2023, publié au Journal officiel israélien (*Reshumut*) le 7 mai 2023.

[33] Voir, par exemple, la résolution du Parlement européen du 25 mars 2021 concernant le rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son entrée en application, 2020/2717(RSP), disponible à l'adresse suivante: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_FR.html.

[34] Voir, par exemple, la position et les conclusions du Conseil relatives à l'application du règlement général sur la protection des données (RGPD), adoptées le 19 décembre 2019, disponibles à l'adresse suivante: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/fr/pdf.

[35] Voir, par exemple, la contribution de l'EDPB à l'évaluation du RGPD au titre de l'article 97, adoptée le 18 février 2020, disponible à l'adresse suivante: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[36] Voir, par exemple, le rapport du groupe d'experts multipartite sur l'évaluation du RGPD, disponible à l'adresse suivante: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&do=groupDetail.groupMeeting&meetingId=21356.

garanties et des limitations appropriées et prévoit des mécanismes de surveillance et de recours dans ce domaine.

Les constatations détaillées concernant chacun des onze pays ou territoires sont présentées dans le document de travail des services de la Commission qui accompagne le présent rapport. Sur la base de ces constatations, la Commission parvient à la conclusion que chacun des onze pays et territoires continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'Union européenne au sens du RGPD, tel qu'interprété par la Cour de justice. Les constatations concernant chacun des pays et territoires concernés sont résumées ci-après.

4.1. Andorre

La Commission salue l'évolution du cadre juridique andorran depuis l'adoption de la décision d'adéquation, y compris les modifications législatives et les activités des organismes de contrôle. En particulier, l'adoption de la loi qualifiée 29/2021 sur la protection des données, qui est entrée en vigueur en mai 2022, a contribué à accroître le niveau de protection des données, car la structure et les principales composantes de cette loi sont étroitement alignées sur le RGPD.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques d'Andorre sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment la Constitution andorrane, la convention européenne des droits de l'homme (CEDH) et la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (la convention 108 et le protocole d'amendement portant création de la convention 108+ modernisée), ainsi que des règles spécifiques de protection des données applicables au traitement des données à caractère personnel dans le cadre de l'application de la législation, qui reprennent pour l'essentiel les éléments clés de la directive (UE) 2016/680[37]. En outre, la législation andorrane impose un certain nombre de conditions et de limitations spécifiques concernant le droit qu'ont les autorités publiques d'accéder aux données à caractère personnel et d'utiliser lesdites données, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que l'Andorre continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

[37] 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.

En ce qui concerne les règles spécifiques de protection des données actuellement applicables au traitement des données par les autorités chargées de faire appliquer la législation, la Commission salue la volonté du législateur andorran de remplacer ces règles par un régime plus complet qui sera encore plus aligné sur les règles applicables au sein de l'UE. La Commission suivra de près l'évolution future de la situation dans ce domaine.

4.2. Argentine

La Commission salue l'évolution du cadre juridique argentin depuis l'adoption de la décision d'adéquation, y compris les modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, l'indépendance de l'autorité argentine de contrôle de la protection des données s'est vue considérablement renforcée par l'adoption du décret nº 746/17, qui confie à l'*Agencia de Acceso a la Información Pública* (ci-après l'«AAIP») la responsabilité de surveiller le respect de la législation relative à la protection des données. En outre, l'AAIP a émis un certain nombre de règlements et d'avis contraignants visant à préciser la façon dont le cadre de protection des données doit être interprété et appliqué dans la pratique, contribuant ainsi à l'actualisation de la législation relative à la protection des données. L'Argentine a également renforcé ses engagements internationaux en matière de protection des données en adhérant, en 2019, à la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et à son protocole additionnel et en ratifiant, en 2023, le protocole d'amendement portant création de la convention 108+ modernisée.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques d'Argentine sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment la Constitution argentine, la convention américaine sur les droits de l'homme, la convention 108 et la convention 108+, ainsi que des règles argentines de protection des données (loi 25.326 du 4 octobre 2000 sur la protection des données à caractère personnel) qui s'appliquent également au traitement des données à caractère personnel par les autorités publiques argentines, notamment pour des raisons de respect de la loi et de sécurité nationale. En outre, la législation argentine impose un certain nombre de conditions et de limitations spécifiques concernant l'accès aux données à caractère personnel et leur utilisation pour des raisons d'application du droit pénal et de sécurité nationale, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que l'Argentine continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

Dans le même temps, la Commission recommande d'inscrire dans la législation les protections qui ont été élaborées au niveau infra-législatif en vue de renforcer la sécurité juridique et de consolider ces exigences. Le projet de loi sur la protection des données qui a récemment été

présenté au Congrès argentin pourrait offrir l'occasion de codifier ces évolutions et de renforcer ainsi davantage le cadre argentin en matière de protection de la vie privée. La Commission suivra de près l'évolution future de la situation dans ce domaine.

4.3. Canada

La Commission salue l'évolution du cadre juridique canadien depuis l'adoption de la décision d'adéquation, y compris les diverses modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, la loi sur la protection des renseignements personnels et les documents électroniques (ci-après la «LPRPDE») a encore été renforcée par différents amendements (concernant, par exemple, les conditions de validité du consentement et les notifications en cas de violation des données), tandis que les principales exigences en matière de protection des données (concernant, par exemple, le traitement des données sensibles) ont été davantage clarifiées par la jurisprudence, ainsi que par les lignes directrices émises par l'organisme fédéral canadien chargé de la protection des données, à savoir le Commissariat à la protection de la vie privée. Dans le même temps, la Commission recommande d'inscrire dans la législation certaines protections qui ont été élaborées au niveau infra-législatif en vue de renforcer la sécurité juridique et de consolider ces exigences. La réforme législative en cours de la LPRPDE pourrait notamment offrir l'occasion de codifier ces évolutions et de renforcer ainsi davantage le cadre canadien en matière de protection de la vie privée. La Commission suivra de près l'évolution future de la situation dans ce domaine.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques du Canada sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre constitutionnel global (la Charte canadienne des droits et libertés), de la jurisprudence, de la législation spécifique réglementant l'accès aux données, ainsi que des règles de protection des données (à savoir, la loi sur la protection des renseignements personnels et toute loi analogue au niveau provincial) qui s'appliquent également au traitement des données à caractère personnel par les autorités publiques canadiennes, notamment pour des raisons de respect de la loi et de sécurité nationale. En outre, le système juridique canadien prévoit des mécanismes effectifs de surveillance et de recours dans ce domaine, notamment grâce à l'extension des droits des personnes concernées et des possibilités de recours pour les ressortissants ou les résidents étrangers.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que le Canada continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE aux destinataires assujettis à la LPRPDE. Comme indiqué ci-dessus, la LPRPDE fait actuellement l'objet d'une réforme législative qui pourrait renforcer davantage les mécanismes de protection de la vie privée, y compris dans des domaines importants pour la décision d'adéquation.

4.4. Îles Féroé

La Commission salue l'évolution du cadre juridique des Îles Féroé depuis l'adoption de la décision d'adéquation, y compris les modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, les Îles Féroé ont modernisé leur cadre de protection des données de manière significative en adoptant la loi relative à la protection des données, qui est entrée en vigueur en 2021 et a permis d'aligner étroitement le régime féroïen sur le RGPD.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques des Îles Féroé sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment le cadre constitutionnel et la CEDH, ainsi que des lois spécifiques régissant l'accès des pouvoirs publics aux données et des règles de protection des données qui s'appliquent au traitement des données à caractère personnel pour des raisons d'application du droit pénal [la loi relative au traitement des données à caractère personnel par les autorités chargées de faire appliquer la législation, qui est entrée en vigueur dans les Îles Féroé en 2022 et transpose la législation adoptée par le Danemark pour mettre en œuvre la directive (UE) 2016/680 dans les Îles Féroé] et de sécurité nationale (énoncées dans la loi sur le service de sécurité et de renseignement). En outre, des mécanismes effectifs de surveillance et de recours sont disponibles dans ce domaine.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que les Îles Féroé continuent d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

4.5. Guernesey

La Commission salue l'évolution du cadre juridique de Guernesey depuis l'adoption de la décision d'adéquation, y compris les modifications législatives et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, Guernesey a modernisé son cadre de protection des données de manière significative en adoptant la loi (du bailliage de Guernesey) sur la protection des données de 2017, qui s'applique depuis 2019 et aligne étroitement le régime de Guernesey sur le RGPD.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques de Guernesey sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment la CEDH et la convention 108, ainsi que des règles de protection des données en vigueur à Guernesey, notamment les dispositions spécifiques relatives au traitement des données à caractère personnel dans le cadre de l'application de la législation énoncées dans l'ordonnance (du bailliage de Guernesey) relative à la protection des données (application de la loi et questions connexes) de 2018. En outre, la législation de Guernesey impose un certain nombre de conditions et de limitations spécifiques concernant

l'accès aux données à caractère personnel et leur utilisation pour des raisons d'application du droit pénal et de sécurité nationale, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que Guernesey continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

4.6. Île de Man

La Commission salue l'évolution du cadre juridique de l'Île de Man depuis l'adoption de la décision d'adéquation, y compris les modifications législatives et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, l'Île de Man a adopté une nouvelle législation en 2018 [la loi relative à la protection des données de 2018, complétée par l'ordonnance relative à la protection des données (application du RGPD) de 2018] qui incorpore la plupart des dispositions du cadre de protection des données de l'UE dans l'ordre juridique de l'Île de Man, tout en apportant quelques ajustements mineurs à certains aspects, notamment pour adapter le cadre au contexte local.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques de l'Île de Man sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment la CEDH et la convention 108, ainsi que des règles de protection des données en vigueur dans l'Île de Man, notamment les dispositions spécifiques relatives au traitement des données à caractère personnel dans le cadre de l'application de la législation énoncées dans l'ordonnance de 2018 relative à la protection des données (application de la directive en matière de protection des données dans le domaine répressif) et les règlements d'exécution de la directive en matière de protection des données dans le domaine répressif de 2018. En outre, la législation de l'Île de Man impose un certain nombre de limitations spécifiques concernant l'accès aux données à caractère personnel et leur utilisation pour des raisons d'application du droit pénal et de sécurité nationale, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que l'Île de Man continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

4.7. Israël

La Commission salue l'évolution du cadre juridique israélien depuis l'adoption de la décision d'adéquation, y compris les modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, Israël a introduit des garanties spécifiques afin de renforcer la protection des données à caractère personnel transférées depuis l'Espace économique européen, en adoptant

le règlement sur la protection de la vie privée (instructions pour les données transférées à Israël depuis l'Espace économique européen), 5783-2023. Israël a également renforcé ses exigences en matière de sécurité des données en adoptant le règlement sur la protection de la vie privée (sécurité des données), 5777-2017, et renforcé l'indépendance de son autorité de contrôle de la protection des données au moyen d'une résolution gouvernementale contraignante.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques d'Israël sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global, notamment la loi fondamentale israélienne, ainsi que de la loi relative à la protection de la vie privée, 5741-1981, et des règlements adoptés en vertu de celle-ci, qui s'appliquent au traitement des données à caractère personnel par les autorités publiques israéliennes, notamment pour des raisons de respect de la loi et de sécurité nationale. En outre, la législation israélienne impose un certain nombre de limitations spécifiques concernant l'accès aux données à caractère personnel et leur utilisation pour des raisons d'application du droit pénal et de sécurité nationale, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut qu'Israël continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

Dans le même temps, la Commission recommande d'inscrire dans la législation les protections qui ont été élaborées au niveau infra-législatif et par la jurisprudence en vue de renforcer la sécurité juridique et de consolider ces exigences. Le projet de loi relatif à la protection de la vie privée (amendement nº 14), 5722-2022, qui a récemment été présenté au Parlement israélien, offre l'occasion de consolider et de codifier ces évolutions, et de renforcer ainsi davantage le cadre israélien en matière de protection de la vie privée. La Commission suivra de près l'évolution future de la situation dans ce domaine.

4.8. Jersey

La Commission salue l'évolution du cadre juridique de Jersey depuis l'adoption de la décision d'adéquation, y compris les modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, Jersey a modernisé son cadre de protection des données de manière significative en adoptant la loi (de Jersey) de 2018 sur la protection des données et la loi (de Jersey) de 2018 sur l'autorité de protection des données, qui sont entrées en vigueur en 2018 et alignent étroitement le régime de Jersey sur le RGPD.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques de Jersey sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements

internationaux, notamment la CEDH et la convention 108, ainsi que des règles de protection des données en vigueur à Jersey, notamment les dispositions spécifiques relatives au traitement des données à caractère personnel dans le cadre de l'application de la législation, énoncées dans la loi (de Jersey) de 2018 sur la protection des données, telle que modifiée par l'annexe 1 de cette loi. En outre, la législation de Jersey impose un certain nombre de limitations spécifiques concernant l'accès aux données à caractère personnel et leur utilisation à des fins d'application du droit pénal et de sécurité nationale, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que Jersey continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

4.9. Nouvelle-Zélande

La Commission salue l'évolution du cadre juridique de la Nouvelle-Zélande depuis l'adoption de la décision d'adéquation, y compris les modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, le régime de protection des données a fait l'objet d'une réforme complète avec l'adoption de la loi de 2020 sur la protection de la vie privée, qui a renforcé davantage la convergence avec le cadre de protection des données de l'UE, notamment en ce qui concerne les règles applicables aux transferts internationaux de données à caractère personnel et les pouvoirs de l'autorité de protection des données (le bureau du commissaire à la vie privée).

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques de Nouvelle-Zélande sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre constitutionnel global (par exemple, la Charte des droits de l'homme) et de la jurisprudence, ainsi que des lois spécifiques régissant l'accès des pouvoirs publics aux données et des dispositions de la loi sur la vie privée, qui s'appliquent également au traitement des données à caractère personnel par les autorités chargées de l'application du droit pénal et de la sécurité nationale. En outre, le système juridique néo-zélandais prévoit différents mécanismes de surveillance et de recours dans ce domaine.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que la Nouvelle-Zélande continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE. La Commission salue également la récente présentation par le gouvernement néo-zélandais au parlement d'un projet de loi visant à modifier la loi de 2020 sur la protection de la vie privée afin de renforcer encore les exigences existantes en matière de transparence. La Commission suivra de près l'évolution future de la situation dans ce domaine.

4.10. Suisse

La Commission salue l'évolution du cadre juridique suisse depuis l'adoption de la décision d'adéquation, y compris les modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, la loi fédérale modernisée sur la protection des données a permis de renforcer davantage la convergence avec le cadre de protection des données de l'UE, notamment en ce qui concerne la protection des données sensibles et les règles relatives aux transferts internationaux de données. La Suisse a également renforcé ses engagements internationaux dans le domaine de la protection des données en ratifiant la convention 108+ en septembre 2023.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques suisses sont soumises à des règles claires, précises et accessibles prévoyant qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment la Constitution fédérale suisse, la CEDH et la convention 108+, ainsi que des règles suisses de protection des données, notamment la loi fédérale sur la protection des données et les règles spécifiques de protection des données applicables aux autorités chargées de l'application du droit pénal (par exemple, le code de procédure pénale) et de la sécurité nationale (par exemple, la loi sur le renseignement). En outre, la législation suisse impose un certain nombre de limitations spécifiques concernant l'accès aux données à caractère personnel et leur utilisation pour des raisons d'application du droit pénal et de sécurité nationale, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales exposées dans le document de travail des services de la Commission, la Commission conclut que la Suisse continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

4.11. Uruguay

La Commission salue l'évolution du cadre juridique uruguayen depuis l'adoption de la décision d'adéquation, y compris les diverses modifications législatives, la jurisprudence et les activités des organismes de surveillance, qui ont contribué à accroître le niveau de protection des données. En particulier, l'Uruguay a modernisé et renforcé sa loi 18.331 de 2008 sur la protection des données à caractère personnel et le recours à l'«habeas data» au moyen de modifications législatives adoptées en 2018 et 2020, qui ont élargi le champ d'application territorial de la législation relative à la protection des données, créé de nouvelles exigences en matière de responsabilité (telles que les analyses d'impact, la protection des données dès la conception et par défaut, la notification des violations de données et la désignation de délégués à la protection des données) et introduit des protections supplémentaires pour les données biométriques. L'Uruguay a également renforcé ses engagements internationaux dans le domaine de la protection des données en adhérant à la convention 108 en 2019 et en ratifiant la convention 108+ en 2021.

Pour ce qui est de l'accès des pouvoirs publics aux données à caractère personnel, les autorités publiques uruguayennes sont soumises à des règles claires, précises et accessibles prévoyant

qu'elles peuvent accéder aux données transférées depuis l'UE et les utiliser ultérieurement pour servir des objectifs d'intérêt public, notamment à des fins d'application du droit pénal et de sécurité nationale. Ces limitations et garanties découlent du cadre juridique global et des engagements internationaux, notamment la Constitution uruguayenne, la convention américaine sur les droits de l'homme, la convention 108 et la convention 108+, ainsi que des règles de protection des données énoncées dans la loi 18.331 sur la protection des données à caractère personnel et le recours à l'«habeas data», qui s'appliquent au traitement des données à caractère personnel par les autorités publiques uruguayennes, notamment à pour des raisons de respect de la loi et de sécurité nationale. En outre, la législation uruguayenne impose un certain nombre de conditions et de limitations spécifiques concernant le droit qu'ont les autorités publiques d'accéder aux données à caractère personnel et d'utiliser lesdites données, et prévoit des mécanismes de surveillance et de recours en la matière.

Sur la base des constatations générales faites dans le cadre de ce premier examen, la Commission conclut que l'Uruguay continue d'assurer un niveau de protection adéquat des données à caractère personnel transférées depuis l'UE.

5. SUIVI ET COOPÉRATION FUTURS

La Commission reconnaît et apprécie grandement l'excellente coopération instaurée avec les autorités compétentes de chacun des pays et des territoires concernés dans le cadre de ce réexamen. La Commission continuera de suivre de près l'évolution des cadres de protection et des pratiques effectives des pays et des territoires concernés. En cas d'évolution, dans un pays ou un territoire, qui serait susceptible d'avoir une incidence négative sur le niveau de protection des données jugé adéquat, la Commission fera, s'il y a lieu, usage des pouvoirs qui lui sont conférés par l'article 45, paragraphe 5, du RGPD aux fins de suspendre, de modifier ou de retirer une décision d'adéquation.

Le présent réexamen confirme que l'adoption d'une décision d'adéquation ne constitue pas une «fin en soi», mais offre l'occasion d'intensifier davantage le dialogue et la coopération avec des partenaires internationaux partageant le même point de vue sur les flux de données et les questions numériques en général. À cet égard, la Commission attend avec intérêt les futurs échanges avec les autorités compétentes afin de renforcer encore la coopération au niveau international en vue de promouvoir des flux de données sûrs et libres, notamment par le biais d'une coopération renforcée en matière d'application de la législation. Afin d'intensifier ce dialogue et de promouvoir l'échange d'informations et d'expériences, la Commission a l'intention d'organiser une réunion à haut niveau en 2024, réunissant des représentants de l'UE et de tous les pays qui bénéficient d'une décision d'adéquation.