EUROPÄISCHE
KOMMISSION

Straßburg, den 20.1.2026
COM(2026) 11 final

2026/0011 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)

{SEC(2026) 11 final} - {SWD(2026) 11 final} - {SWD(2026) 12 final}

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Seit der Annahme des Rechtsakts zur Cybersicherheit im Jahr 2019 hat sich die Bedrohungslage im Bereich der Cybersicherheit in einem zunehmend komplexen geopolitischen Umfeld erheblich verändert[1]. Cyberangriffe gegen kritische Infrastrukturen, Unternehmen und die breite Öffentlichkeit haben zugenommen und sind immer ausgefeilter geworden, wobei Ransomware-Vorfälle im Mittelpunkt stehen[2]. Neu aufkommende Technologien wie künstliche Intelligenz (KI) und Quanteninformatik verändern die Abwehrinstrumente und die Taktik der Gegner. In seinem **Bericht „Die Zukunft der europäischen Wettbewerbsfähigkeit“** aus dem Jahr 2024 betonte Mario Draghi, dass die Sicherheit erhöht und Abhängigkeiten verringert werden müssen, da dies einer der wichtigsten Aktionsbereiche in der Europäischen Union ist[3]. Sowohl durch die Europäische Strategie für eine Union der Krisenvorsorge[4] als auch die Europäische Strategie für die innere Sicherheit (ProtectEU)[5] ist die Cybersicherheit in den Mittelpunkt der Resilienzagenda der Union gerückt. In diesen Strategien wird anerkannt, dass anhaltende Cybersicherheitsbedrohungen nicht nur technische Herausforderungen, sondern auch strategische Risiken für unsere Demokratie, Wirtschaft und Lebensweise darstellen. Ebenso werden in der Mitteilung über die Stärkung der wirtschaftlichen Sicherheit der EU[6] die Verhinderung des Zugangs zu sensiblen Informationen und Daten, die die wirtschaftliche Sicherheit der Union aushöhlen könnten, und die Verhinderung und Entschärfung von Störungen kritischer Infrastrukturen der Union, die die Wirtschaft der Union beeinträchtigen, als vorrangige Ziele genannt, bei denen wirksame Cybersicherheitsmaßnahmen eine entscheidende Rolle spielen.

Vor diesem Hintergrund **gibt es vier Hauptprobleme**, die mit der vorgeschlagenen Überarbeitung des Rechtsakts zur Cybersicherheit angegangen werden sollen: i) die Diskrepanz zwischen dem politischen Rahmen der Union für die Cybersicherheit und den Bedürfnissen der Interessenträger angesichts einer zunehmend feindseligen Bedrohungslage, ii) die ins Stocken geratene Umsetzung des europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF), iii) die Komplexität und Vielfalt der Cybersicherheitsstrategien, die sich auf die Cyberabwehr der Union auswirken, und iv) die Erhöhung der Sicherheitsrisiken in den IKT-Lieferketten.

Ausgehend von den ermittelten Hauptproblemen bestehen die **zwei allgemeinen Ziele** der Maßnahme darin, die Cybersicherheitskapazitäten und die Resilienz zu erhöhen und eine Fragmentierung im gesamten Binnenmarkt zu verhindern, und zwar durch

- einen Beitrag zur Stärkung der Governance der Union im Bereich Cybersicherheit sowie einen Beitrag dazu, dass die einschlägigen Organe, Behörden und anderen

---

1 ENISA, ENISA Threat Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

2 ENISA, ENISA Threat Landscape 2025.

3 Europäische Kommission, „Die Zukunft der europäischen Wettbewerbsfähigkeit“, (https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_de).

4 JOIN(2025) 130 final.

5 COM(2025) 148 final.

6 JOIN(2025) 977 final.

Interessenträger besser darauf vorbereitet sind, Cybersicherheitsbedrohungen koordiniert und wirksam zu verhindern, zu erkennen und darauf zu reagieren, und

- Unterstützung der Entwicklung, Umsetzung und Einführung gemeinsamer Cybersicherheitsinstrumente der Union, wie z. B. Zertifizierungssysteme, und Bereitstellung harmonisierter Rahmen zum Aufbau von Vertrauen und Interoperabilität zwischen den Mitgliedstaaten.

Diese allgemeinen Ziele sind die Antwort auf die wichtigsten Herausforderungen, die im Rahmen der Problemstellung ermittelt wurden. Sie spiegeln das übergeordnete politische Ziel wider, die Governance im Bereich der Cybersicherheit in der Union zu stärken und die Entwicklung eines sicheren, widerstandsfähigen und wettbewerbsfähigen digitalen Binnenmarkts zu unterstützen.

Um zur Verwirklichung der genannten allgemeinen Ziele beizutragen, werden mit dieser Maßnahme die folgenden **spezifischen Ziele (SPO)** verfolgt:

- Behebung der Diskrepanz zwischen dem politischen Rahmen der Union für die Cybersicherheit und den Bedürfnissen der Interessenträger:
  - SPO1: Schaffung der Kapazitäten für die wirksame Umsetzung der Cybersicherheitspolitik der Union und für eine kontinuierliche operative Zusammenarbeit, die eine strukturiertere Zusammenarbeit zwischen den Mitgliedstaaten ermöglicht;
  - SPO2: Entwicklung und Umsetzung von Mitteln und Mechanismen zur wirksamen Unterstützung und Deckung des Bedarfs der Mitgliedstaaten, der Industrie und anderer Interessenträger;
- Maßnahmen zur Erhöhung der Inanspruchnahme und Wirksamkeit des ECCF:
  - SPO3: Schaffung der Voraussetzungen für eine schnellere Bereitstellung von Systemen für die Cybersicherheitszertifizierung auf der Grundlage des Marktbedarfs, indem der Umfang des ECCF ausgeweitet wird, eine wirksame Systempflege und flexible Verfahren sichergestellt werden und die Transparenz erhöht wird;
- Verringerung der Fragmentierung der Rechtsvorschriften und der Komplexität horizontaler und sektoraler Regelungen:
  - SPO4: Schaffung von Mechanismen und Bedingungen, um die Einhaltung der Anforderungen an die Cybersicherheit zu erleichtern und so ihre Umsetzung kohärenter und wirksamer zu gestalten;
- Bewältigung von Cybersicherheitsrisiken in der Lieferkette:
  - SPO5: Verringerung der Risiken bei kritischen IKT-Lieferketten von Einrichtungen, die in Drittländern, für die Cybersicherheitsbedenken bestehen, niedergelassen sind oder von Einrichtungen in diesen Drittländern kontrolliert werden (Hochrisikoanbieter), und Verringerung kritischer Abhängigkeiten durch die Entwicklung eines kohärenten und wirksamen Rahmens auf EU-Ebene zur Bewältigung von Risiken für die Sicherheit von IKT-Lieferketten.

Die Überarbeitung des Rechtsakts zur Cybersicherheit fällt unter das **Programm zur Gewährleistung der Effizienz und Leistungsfähigkeit der Rechtsetzung (REFIT)**. Sie

trägt in hohem Maße zu mehr Klarheit, zur Beseitigung von Ineffizienzen und zur Angleichung von Verfahren verschiedener Rechtsrahmen bei. Die Überarbeitung des Rechtsakts zur Cybersicherheit verhilft zu einem reibungslosen Funktionieren des Binnenmarkts und gewährleistet gleichzeitig die Sicherheit und strategische Autonomie der Union.

Konkret wird eine vollständige Reform des Mandats der Agentur der Europäischen Union für Cybersicherheit (ENISA) vorgeschlagen, um die Umsetzung politischer Maßnahmen wirksam zu unterstützen und einen Mehrwert im Hinblick auf die Unterstützung der operativen Zusammenarbeit zwischen den Mitgliedstaaten zu schaffen.

Angesichts der zunehmenden Bedrohungen und Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollen mit dem Vorschlag die finanziellen und personellen Ressourcen der ENISA erhöht werden, damit sie ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung bei der Verteidigung des digitalen Ökosystems der Union gerecht werden kann, sodass die ENISA die ihr mit diesem Vorschlag übertragenen Aufgaben wirksam erfüllen kann.

Die Überarbeitung wird auch dazu beitragen, fragmentierte Praktiken zu beseitigen, die Koordinierung zu verbessern und gleichzeitig die Befolgungs- und Betriebskosten langfristig zu senken. Mit dem Vorschlag wird der derzeitige Rechtsakt zur Cybersicherheit aufgehoben und ein reformierter ECCF eingeführt. Dadurch steht ein wirksameres und effizienteres Instrument zur Verfügung, das sowohl das Vertrauen zwischen Unternehmen, der breiten Öffentlichkeit und den Behörden fördert als auch die Einhaltung der einschlägigen Rechtsvorschriften der Union erleichtert. Durch ein überarbeitetes Governance-Modell und berechenbarere, kohärentere und flexiblere Zertifizierungsverfahren sorgt der Vorschlag für mehr Effizienz, sodass Systeme schneller entwickelt und umgesetzt werden können.

Größere Synergien mit den bestehenden einschlägigen Rechtsrahmen der Union werden die Zertifizierung als Einhaltungsinstrument für Unternehmen fördern und den Verwaltungsaufwand für Konformitätsbewertungsstellen verringern, die im Rahmen mehrerer Rechtsakte im Bereich der Cybersicherheit tätig sind. Dadurch, dass der Umfang des ECCF ausgeweitet und die Entwicklung eines Systems für die Cyberabwehr von Einrichtungen ermöglicht wird, werden mit dem Vorschlag außerdem die Befolgungskosten für Einrichtungen gesenkt, die den einschlägigen Rechtsvorschriften der Union im Bereich der Cybersicherheit unterliegen, angefangen bei Einrichtungen, die in den Anwendungsbereich der NIS-2-Richtlinie fallen. Dieser Ansatz wird die regulatorischen Verpflichtungen für Einrichtungen, die mehreren Einhaltungsanforderungen unterliegen, erheblich vereinfachen und eine wirksamere Nutzung der Ressourcen durch die nationalen Behörden gewährleisten. Zusätzlich zu dieser Überarbeitung soll durch einen Vorschlag für eine Richtlinie mit gezielten Änderungen der NIS-2-Richtlinie die Einhaltung bestimmter Aspekte des Cybersicherheitsrahmens vereinfacht und eine gestraffte und kohärente Umsetzung gewährleistet werden, auch in Bezug auf den Umfang, die Begriffsbestimmungen, die Meldung von Ransomware-Vorfällen und die Beaufsichtigung von Einrichtungen, die grenzübergreifende Dienste erbringen.

Mit der neuen Verordnung wird auch ein harmonisierter Rahmen für die Bewältigung nicht technischer Risiken geschaffen, die sich auf die IKT-Lieferketten auswirken, wodurch die derzeit inkohärenten Ansätze in den Mitgliedstaaten einheitlicher gestaltet werden.

Zusammengenommen stellen diese Aspekte eine erhebliche Vereinfachung und Modernisierung des Rechtsrahmens der Union für die Cybersicherheit dar, was vollständig mit den REFIT-Grundsätzen der Klarheit, Effizienz und Bereitschaft für den digitalen Wandel im Einklang steht.

- **Kohärenz mit den bestehenden Vorschriften in diesem Bereich**

Die Union hat ihre rechtlichen und politischen Instrumente durch die Annahme einer Reihe von Rechtsinstrumenten und politischen Maßnahmen erweitert: i) Die NIS-2-Richtlinie dient der Stärkung der Cybersicherheit kritischer Infrastrukturen; ii) physische Sicherheitsmaßnahmen sind in ihrer „Schwesterrichtlinie", der Richtlinie über die Resilienz kritischer Einrichtungen, definiert; iii) mit der Cyberresilienzverordnung wird die Cybersicherheit von Produkten verbessert; iv) mit der Cybersolidaritätsverordnung werden EU-weite Reaktionsfähigkeiten aufgebaut; v) der EU-Cyberkonzeptentwurf[7] fördert die Zusammenarbeit bei der Krisenbewältigung auf EU-Ebene, in deren Rahmen die Kommission und der Hohe Vertreter/die Hohe Vertreterin eine Schlüsselrolle bei der Vorbereitung und Reaktion auf große Cybersicherheitsvorfälle spielen; vi) das Instrumentarium für die 5G-Cybersicherheit (5G-Instrumentarium) unterstützt die Cybersicherheit in 5G-Netzen; vii) der europäische Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern[8] trägt zur Verbesserung von deren Cybersicherheit bei und viii) die Akademie für Cybersicherheitskompetenzen[9] befasst sich mit der wachsenden Herausforderung des Fachkräftemangels im Bereich der Cybersicherheit.

Der genannte Rechtsrahmen für die Cybersicherheit wurde durch sektorspezifische Rechtsvorschriften ergänzt, nämlich die Verordnung über die digitale operationale Resilienz im Finanzsektor (DORA-Verordnung), den Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse (NCCS) für den Teilsektor Strom und die Vorschriften für die Informationssicherheit (Teil-IS[10]) für den Teilsektor Luftverkehr.

Die Überarbeitung des Rechtsakts zur Cybersicherheit steht im Einklang mit den Bestimmungen der NIS-2-Richtlinie hinsichtlich der Rolle der ENISA bei der Unterstützung der Umsetzung der genannten Richtlinie und stärkt diese, auch in Bezug auf die Unterstützung der operativen Zusammenarbeit; sie steht zudem im Einklang mit der Cyberresilienzverordnung, auch hinsichtlich des Überblicks über und des Umgangs mit Schwachstellen im gesamten Binnenmarkt, und sorgt für einen erhöhten Mehrwert gemeinsamer Lageerfassung. Was den ECCF betrifft, so steht die Überarbeitung des Rechtsakts zur Cybersicherheit mit den die Ziele für die Produktsicherheit und den Umgang mit Schwachstellen betreffenden Bestimmungen der Cyberresilienzverordnung sowie mit dem neuen Rechtsrahmen für die Akkreditierung im Einklang. Darüber hinaus gibt es starke Synergien, die sich aus der Entwicklung der Zertifizierung der Cyberabwehr für die NIS-2-Richtlinie ergeben und möglicherweise die Einhaltung anderer einschlägiger Rechtsakte der Union wie der Datenschutz-Grundverordnung (DSGVO) erleichtern werden, unbeschadet ihrer spezifischen Zertifizierungsanforderungen. Darüber hinaus unterstützt der horizontale

---

7 COM(2025) 66 final.
8 COM(2025) 10 final.
9 COM(2023) 207 final.
10 Durchführungsverordnung (EU) 2023/203 der Kommission und Delegierte Verordnung (EU) 2022/1645 der Kommission.

Rahmen, der sich mit Cybersicherheitsrisiken in IKT-Lieferketten befasst, das übergeordnete Ziel der NIS-2-Richtlinie, ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union zu schaffen, und stützt sich auf den risikobasierten Ansatz der NIS-2-Richtlinie.

Darüber hinaus bietet die Überarbeitung des Rechtsakts zur Cybersicherheit in Verbindung mit dem Vorschlag für eine Richtlinie mit gezielten Änderungen der NIS-2-Richtlinie zur Vereinfachung die erforderlichen Instrumente, um diesen umfassenden Rahmen im Hinblick auf die erwarteten Ergebnisse wirksamer und effizienter zu gestalten, eine ausgeprägtere europäische Dimension zu schaffen und die verbleibenden Regulierungslücken zu schließen.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Die Überarbeitung des Rechtsakts zur Cybersicherheit würde die Richtlinie über die Resilienz kritischer Einrichtungen ergänzen, die Erwägungen zu Lieferketten als Teil der Maßnahmen zur Steigerung der Resilienz kritischer Einrichtungen enthält. Darüber hinaus würden dadurch künftige Initiativen ergänzt, so z. B. i) der Rechtsakt über Cloud- und KI-Entwicklung, mit dem unter anderem Abhilfe dagegen geschaffen werden soll, dass die Union nicht über ein eigenes wettbewerbsfähiges Angebot an Cloud-Computing-Diensten in ausreichendem Umfang für hochkritische Anwendungsfälle oder Sektoren verfügt; ii) der Vorschlag für die Verordnung über digitale Netze; iii) die bevorstehende Überarbeitung der Verordnung (EU) 2023/1781[11], iv) der Rahmen für die Vergabe öffentlicher Aufträge[12], der derzeit bewertet wird[13], und der Vorschlag für eine Verordnung zur Vereinfachung des digitalen Rechtsrahmens (Digital-Omnibus-Verordnung)[14], durch den die ENISA verpflichtet wird, eine zentrale Anlaufstelle für die Meldung von Sicherheitsvorfällen zu entwickeln, über die Einrichtungen ihren Pflichten zur Meldung von Sicherheitsvorfällen gemäß mehreren Rechtsakten gleichzeitig nachkommen können. Darüber hinaus würde die Position der Behörden und Betreiber der Union bei der Zusammenarbeit mit den Partnern im südlichen Mittelmeerraum gestärkt, insbesondere durch die Förderung der Vernetzung über sichere und vertrauenswürdige digitale Infrastrukturen im gesamten Mittelmeerraum, was eines der grundlegenden Ziele des Pakts für den Mittelmeerraum ist.

Die Überarbeitung des Rechtsakts zur Cybersicherheit steht auch im Einklang mit den strategischen Dokumenten der Union, insbesondere mit dem Rahmen für die Sicherheit der IKT-Lieferketten. In der ProtectEU-Strategie erklärte die Kommission außerdem, dass ein harmonisierter Ansatz für die Sicherheit der IKT-Lieferketten der derzeitigen Fragmentierung des Binnenmarkts aufgrund unterschiedlicher Ansätze auf nationaler Ebene entgegenwirken, kritische Abhängigkeiten vermeiden und von Hochrisikoanbietern ausgehende Risiken für IKT-Lieferketten verringern kann, wodurch kritische Infrastrukturen gesichert werden. Auch in der Strategie für wirtschaftliche Sicherheit[15] wird betont, dass die Wirtschaft und die Lieferketten der EU widerstandsfähiger werden müssen, um die Wettbewerbsfähigkeit der EU zu fördern. Dass Unterbrechungen der Lieferketten und Cyberangriffen entgegengewirkt

---

11 Verordnung (EU) 2023/1781 des Europäischen Parlaments und des Rates vom 13. September 2023 zur Schaffung eines Rahmens für Maßnahmen zur Stärkung des europäischen Halbleiter-Ökosystems und zur Änderung der Verordnung (EU) 2021/694 (Chip-Gesetz) (ABl. L 229 vom 18.9.2023, S. 1).

12 Insbesondere die Richtlinien 2014/23/EU, 2014/24/EU und 2014/25/EU.

13 Europäische Kommission, Kommission veröffentlicht Aufforderung zur Stellungnahme und leitet öffentliche Konsultation zur Bewertung der Richtlinien über die Vergabe öffentlicher Aufträge ein, https://single-market-economy.ec.europa.eu/news/commission-launches-call-evidence-and-public-consultation-evaluation-public-procurement-directives-2024-12-13_de.

14 COM(2025) 837 final.

15 JOIN(2023) 20 final.

werden muss, wurde auch in der Strategie für eine Union der Krisenvorsorge und im Weißbuch zur europäischen Verteidigung[16] betont. Darüber hinaus entspricht der Vorschlag, wie bereits erwähnt, dem Bericht über die Zukunft der europäischen Wettbewerbsfähigkeit von Mario Draghi. Zudem steht die Überarbeitung des Rechtsakts zur Cybersicherheit betreffend die Sicherheit der IKT-Lieferketten mit der kürzlich angenommenen Gemeinsamen Mitteilung an das Europäische Parlament und den Rat über die Stärkung der wirtschaftlichen Sicherheit der EU[17] im Einklang.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

• Rechtsgrundlage

Rechtsgrundlage dieses Vorschlags ist Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV). Artikel 114 AEUV regelt den Erlass von Maßnahmen, die die Errichtung und das Funktionieren des Binnenmarkts gewährleisten sollen. Die Verordnung (EU) 2019/881 über die ENISA und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik[18], gemeinhin als Rechtsakt zur Cybersicherheit bekannt, wurde ursprünglich auf der Grundlage dieser Bestimmung erlassen.

Im Bereich der Cybersicherheit der IKT-Lieferketten wirkt sich die Fragmentierung der nationalen Rahmen zur Bewältigung nicht technischer Risikofaktoren negativ auf das Funktionieren des Binnenmarkts aus, da die Unterschiede zwischen den nationalen Ansätzen letztlich zu einer höheren Anfälligkeit einiger Mitgliedstaaten führen könnten, was potenzielle Spillover-Effekte in der gesamten Union mit sich bringen und sich auf die allgemeine Resilienz und auch auf die Vertrauenswürdigkeit auswirken könnte.

Angesichts der sich wandelnden Cybersicherheitsbedrohungen und der zunehmenden gegenseitigen Abhängigkeiten der digitalen Systeme der Mitgliedstaaten ist Artikel 114 AEUV auch weiterhin die begründete Rechtsgrundlage für die Überarbeitung des Rechtsakts zur Cybersicherheit. Die vorgeschlagene Verordnung spiegelt die jüngsten Entwicklungen im Bereich der Rechtsvorschriften für die Cybersicherheit wider, insbesondere vor dem Hintergrund der wachsenden Zuständigkeiten der ENISA und des immer größeren Umfangs von Zertifizierungen und Risikomanagement.

• Subsidiarität (bei nicht ausschließlicher Zuständigkeit)

Das Subsidiaritätsprinzip erfordert eine Bewertung der Notwendigkeit und des Mehrwerts des Handelns der Union. Die Einhaltung des Subsidiaritätsprinzips in diesem Bereich wurde bereits bei der Annahme des derzeitigen Rechtsakts zur Cybersicherheit anerkannt.

Wie bereits die Analyse im Zusammenhang mit dem genannten Rechtsakt ergeben hat, ist ein Tätigwerden der Union unerlässlich, da Cybersicherheitsbedrohungen und die damit verbundenen Herausforderungen nicht an den Grenzen der Mitgliedstaaten haltmachen. Fragmentierte nationale Lösungen haben sich als unzureichend erwiesen, um Vertrauen und Koordinierung im gesamten Markt zu erreichen. Ein überarbeiteter Rechtsrahmen der Union ist erforderlich, um Hindernisse zu beseitigen, eine einheitliche Umsetzung zu gewährleisten und die Mitgliedstaaten in einem immer komplexeren Regelungs- und Bedrohungsumfeld zu unterstützen. Cybersicherheit ist ein Thema von gemeinsamem Interesse für die Union.

---

16 JOIN(2025) 120 final.
17 JOIN(2025) 977 final.
18 Verordnung (EU) 2019/881 – DE – EUR-Lex.

Die Maßnahmen, die Gegenstand der vorgeschlagenen Verordnung sind, bieten einen klaren Mehrwert, da sie Harmonisierung, Rechtsklarheit und koordinierte Reaktionen auf Herausforderungen im Bereich der Cybersicherheit fördern.

Die Aufgaben der ENISA wurden durch nachfolgende Rechtsvorschriften stetig erweitert, ohne dass ihre grundlegenden Zuständigkeiten und ihre Ressourcen angepasst wurden. Dies hat Ineffizienzen hervorgebracht und dazu geführt, dass die Kernaufgaben zur Unterstützung der Mitgliedstaaten nicht ausreichend priorisiert wurden. Daher sollen mit dem Vorschlag für ein Tätigwerden die derzeitigen Aufgaben zielgerichteter ausgestaltet und priorisiert werden, damit das Mandat der ENISA gestärkt wird und sie als zentrale Anlaufstelle für Sachkenntnis im Bereich der Cybersicherheit auf Unionsebene fungieren kann. Diesbezüglich gibt es, was die Subsidiarität betrifft, keinen wesentlichen Unterschied im Vergleich zum Rechtsakt zur Cybersicherheit. Darüber hinaus führen unterschiedliche nationale Zertifizierungssysteme und unterschiedliche Regulierungsansätze der Mitgliedstaaten zu einer Marktfragmentierung und zusätzlichem Aufwand bei der Einhaltung der Vorschriften, wodurch die Wettbewerbsfähigkeit untergraben wird.

Der neue Vorschlag sieht auch neue Maßnahmen in Bezug auf Lieferkettenstrategien und Vereinfachungsbemühungen auf Unionsebene vor. Er stärkt die Sicherheit der Lieferketten und des Cybersicherheitssektors in der Union weiter und erhöht die Abwehrbereitschaft und Resilienz der Mitgliedstaaten und der Industrie.

Abhängigkeiten von Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder von einem solchen Drittland, einer in diesem Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert werden (Hochrisikoanbieter), betreffen Einrichtungen in der gesamten Union, und schwerwiegende Cybersicherheitsvorfälle in der Lieferkette breiten sich häufig über nationale Grenzen hinweg aus. Darüber hinaus würde angesichts des grenzübergreifenden Charakters der IKT-Lieferketten eine Fragmentierung der Einhaltungsanforderungen im Binnenmarkt die Rechtssicherheit für Einrichtungen untergraben. Außerdem ist in den Vorschlägen für den mehrjährigen Finanzrahmen (MFR) der Ausschluss von Hochrisikoanbietern vorgesehen, um die Integrität des Haushalts und die Sicherheitsinteressen der EU zu wahren. Der in dieser Verordnung enthaltene Rahmen für die Lieferketten umfasst einen Mechanismus zur Ermittlung von Ländern, für die Cybersicherheitsbedenken bestehen; diese Aufgabe kann nur auf EU-Ebene wirksam wahrgenommen werden. Was die Sicherheit der IKT-Lieferketten betrifft, wird nur ein Tätigwerden auf EU-Ebene unionsweit das gleiche Mindestsicherheitsniveau und die notwendige Harmonisierung der Ansätze gewährleisten.

Mit dieser Überarbeitung wird der Zweck des Rechtsakts zur Cybersicherheit beibehalten und weiter gestärkt. Die Mitgliedstaaten können dies nicht in ausreichendem Maß erreichen; es kann im Einklang mit Artikel 5 des Vertrags über die Europäische Union auf Unionsebene besser verwirklicht werden.

- **Verhältnismäßigkeit**

Die vorgeschlagenen Maßnahmen gehen nicht über das zur Erreichung der politischen Ziele des Vorschlags erforderliche Maß hinaus. Zudem werden weitere einzelstaatliche Maßnahmen in Angelegenheiten der nationalen Sicherheit durch den Umfang der Unionsmaßnahmen nicht beeinträchtigt. Ein Tätigwerden der Union ist daher aus Gründen der Subsidiarität und Verhältnismäßigkeit gerechtfertigt.

Mit dem Vorschlag sollen das Mandat der ENISA und das Verfahren für die Entwicklung, Annahme und Aufrechterhaltung europäischer Cybersicherheitszertifikate rechtlich besser widergespiegelt werden. Der Vorschlag umfasst zwar bestimmte neue Aufgaben für die ENISA, diese zielen jedoch darauf ab, die Mitgliedstaaten in den Bereichen zu unterstützen, in denen erhebliche Lücken festgestellt wurden. Die ENISA wird die Computer-Notfallteams der Mitgliedstaaten nicht ersetzen. Was den ECCF betrifft, so bleibt die Zertifizierung freiwillig und kann Einrichtungen dabei helfen, die Einhaltung der Cybersicherheitsanforderungen der Union nachzuweisen. Mit diesem Ansatz wird sichergestellt, dass der Grundsatz der Verhältnismäßigkeit gewahrt bleibt.

In Bezug auf die vorgeschlagenen Lösungen für die Sicherheit der IKT-Lieferketten sieht der Rahmen vor, Nachweise dafür zu sammeln, was wichtige Assets sind und welche Maßnahmen verhältnismäßig und erforderlich wären, um die Risiken bei kritischen Lieferketten zu verringern. Vor der Festlegung dieser Maßnahmen wird eine Bewertung der wirtschaftlichen Auswirkungen durchgeführt, bei der unter anderem die wirtschaftliche Durchführbarkeit, auf dem Markt verfügbare Alternativen und der Lebenszyklus der jeweiligen Produkte untersucht werden. Diese Bewertung wird Aufschluss darüber geben, welche risikobasierten Maßnahmen erforderlich und am besten geeignet sind.

- **Wahl des Instruments**

Mit dem vorliegenden Vorschlag wird die Verordnung (EU) 2019/881 überarbeitet, in der das derzeitige Mandat und die derzeitigen Aufgaben der ENISA und des ECCF enthalten sind. Daher lassen sich das überarbeitete Mandat der ENISA und Änderungen des ECCF am besten im Rahmen desselben Rechtsinstruments, konkret einer Verordnung, festlegen. Der vorgeschlagene Rechtsakt enthält auch einen wirksamen Rahmen auf EU-Ebene zur Bewältigung von Sicherheitsrisiken in den IKT-Lieferketten. Durch eine Verordnung ließen sich die festgestellten Probleme wirksamer angehen und die formulierten Ziele besser erreichen, da nur ein Tätigwerden auf EU-Ebene ein einheitliches Sicherheitsniveau in der gesamten Union und die notwendige Harmonisierung der Ansätze gewährleistet. Bei einer Richtlinie für ein solches Tätigwerden könnte der Umsetzungsprozess zu viel Ermessensspielraum auf nationaler Ebene lassen, was zu Uneinheitlichkeit bestimmter grundlegender Cybersicherheitsanforderungen, Rechtsunsicherheit, einer weiteren Fragmentierung oder sogar diskriminierenden grenzübergreifenden Situationen führen könnte.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Die Europäische Kommission hat gemäß Artikel 67 der Verordnung (EU) 2019/881 die Relevanz, Wirkung, Wirksamkeit, Effizienz, Kohärenz und den Mehrwert der ENISA und des ECCF unter Berücksichtigung der technologischen Entwicklung und des sich wandelnden Regulierungsumfelds bewertet. Diese im Dezember 2024 abgeschlossene Bewertung erstreckte sich auf den Zeitraum von 2017 bis 2023 und zielte darauf ab, das Mandat und die Tätigkeiten der ENISA zu überprüfen und die Rolle des ECCF bei der Förderung eines sicheren Cyberumfelds in der gesamten EU zu bewerten. Die wichtigsten Ergebnisse lassen sich wie folgt zusammenfassen:

- **Relevanz:** Die Bedeutung der ENISA im Bereich der Cybersicherheit zeigt sich in ihrer Reaktionsfähigkeit auf die sich wandelnden Bedürfnisse der Interessenträger und ihrer Fähigkeit zur Anpassung an ein sich änderndes Umfeld. Insgesamt sind die

Interessenträger zwar zufrieden, doch die Wirkung der ENISA ließe sich erhöhen. Dies kann erreicht werden, indem die Unterstützung und die Sichtbarkeit für verschiedene Sektoren verbessert werden, insbesondere für kleine und mittlere Unternehmen (KMU), die häufig mit Cybersicherheitsanforderungen zu kämpfen haben. Ein optimierter Einsatz von Ressourcen und eine klarere Abstimmung mit nationalen Behörden sind von entscheidender Bedeutung. Durch die Neugewichtung der Prioritäten und die Optimierung der vorhandenen Ressourcen wird die ENISA besser an die dynamischen Anforderungen in der europäischen Cybersicherheitslandschaft angepasst.

Für den ECCF gilt trotz der vielversprechenden Ausgangslage nach wie vor, dass mehr Potenzial in ihm steckt, als die Praxis bislang gezeigt hat, da erst ein einziges Zertifizierungssystem seit Kurzem in Betrieb ist. Der Rahmen soll sich nahtlos in andere Rechtsakte der Union einfügen, um Verfahren zu straffen und grenzübergreifenden Handel zu erleichtern. Seine Bedeutung wird in Bereichen mit hohen Sicherheitsanforderungen wie Cloud-Diensten und 5G-Infrastrukturen deutlich.

- **Wirksamkeit:** Die ENISA hat ihren Auftrag erfolgreich erfüllt, indem sie fast alle geplanten Outputs erbracht und Flexibilität und Resilienz in Krisen wie der COVID-19-Pandemie und dem russischen Angriffskrieg gegen die Ukraine unter Beweis gestellt hat. Um die Effizienz zu steigern, sind jedoch eine bessere Priorisierung, eine klare Fokussierung und eine strategische Ressourcenzuweisung erforderlich. Ein flexiblerer Ansatz für die interne Führung ist unerlässlich, um mit den sich wandelnden Cybersicherheitsanforderungen Schritt zu halten und Verzögerungen zu minimieren.

  Mit dem ECCF sollte die Cybersicherheitszertifizierung in der gesamten Union harmonisiert werden, allerdings war er mit erheblichen Herausforderungen konfrontiert, darunter Verfahrensbeschränkungen und Fragmentierung, die zu Verzögerungen und Ineffizienzen führten, wie z. B. die verspätete Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC). Externe Faktoren wie geopolitische Spannungen und die COVID-19-Pandemie erschwerten die Verwirklichung der Ziele des ECCF weiter und machten deutlich, dass anpassbare Maßnahmen und eine kohärente Ressourcenzuweisung zwischen den Interessenträgern erforderlich sind, um eine einheitliche und wirksame Cybersicherheitszertifizierung zu erreichen. Trotz dieser Hindernisse wurden positive Ergebnisse erzielt – insbesondere bei der Sensibilisierung der Mitgliedstaaten für die Bedeutung und die Komplexität der Cybersicherheitszertifizierung.

- **Effizienz:** Die ENISA arbeitete in ihrem matrixbasierten Organisationsrahmen effizient und legte großen Wert auf Zusammenarbeit und Aufgabenpriorisierung. Sie stand jedoch vor Herausforderungen bei der Deckung des steigenden Bedarfs und der Besetzung von Stellen für hoch qualifiziertes Personal – verschärft durch den weltweiten Mangel an IT-Fachkräften –, was zu Verzögerungen und hoher Arbeitsbelastung führte. Um diese Probleme zu beheben, könnte die ENISA ihr internes Personal optimieren und Ressourcen wirksam umschichten, indem sie strategische Anpassungen vornimmt, wie bei der Umschichtung von Ressourcen zur Stärkung der Aktion zur Förderung der Cybersicherheit im Jahr 2022. Darüber hinaus würden eine bessere Mittelbewirtschaftung und geringere Verwaltungsausgaben die operative Effizienz der Agentur weiter verbessern.

Die Effizienz des ECCF stand in der Kritik, da die Annahme von Systemen für die Cybersicherheitszertifizierung sehr lang dauerte und sehr komplex war, sodass das erste System erst Anfang 2024, also fast fünf Jahre nach Erlass des Rechtsakts zur Cybersicherheit, angenommen wurde. Politische und technische Herausforderungen wie Debatten über Datensouveränität und Schwierigkeiten bei der Umsetzung von Entwürfen in Rechtsakte sorgten ebenfalls für Verzögerungen. Zudem wurden Fortschritte durch politische Herausforderungen und technische Anforderungen behindert, wie sich beim Cloud-Zertifizierungssystem der EU (EUCS) und dem EU5G-System zeigte. Trotz dieser Ineffizienzen führte der Rahmen zu mehreren positiven Entwicklungen. Dennoch besteht nach wie vor Verbesserungsbedarf bei der Einbeziehung der Interessenträger und bei der internen Governance, um ein optimales Funktionieren und einen optimalen strategischen Beitrag zu gewährleisten.

- **Kohärenz:** Die Kohärenz der ENISA wird durch eine umfassende Einbeziehung der Interessenträger und die Angleichung an die jüngsten Rechtsrahmen unterstützt. Um die Kohärenz und die Ressourcenzuweisung zu verbessern, ist es jedoch von entscheidender Bedeutung, Synergien mit anderen Einrichtungen der Union, wie dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC), und nationalen Behörden zu verbessern. Darüber hinaus gilt es, an der internen Kommunikation und dem Ressourcenmanagement innerhalb der ENISA sowie der transparenten Interaktion mit privaten Interessenträgern zu arbeiten. Eine klare Abgrenzung der Aufgaben der ENISA im Einklang mit der Cyberresilienzverordnung und der NIS-2-Richtlinie wird sowohl die Effizienz als auch die regulatorische Kohärenz verbessern.

  Beim ECCF ist die uneingeschränkte Kohärenz mit anderen Rechtsinstrumenten der Union, einschließlich der NIS-2-Richtlinie und der Cyberresilienzverordnung, entscheidend, um ein einheitliches Cybersicherheitskonzept zu gewährleisten. Theoretisch ist der ECCF zwar an diese Gesetzgebungsmaßnahmen angeglichen, in der Praxis erweist sich die Integration jedoch nach wie vor als komplex und erfordert eine sorgfältige Beaufsichtigung. Die Umsetzung des angenommenen EUCC-Systems innerhalb des Rahmens der Cyberresilienzverordnung wird hier ein wichtiger Test sein.

- **EU-Mehrwert:** Die ENISA hat durch die Förderung der Zusammenarbeit und die Angleichung von Verfahren einen wesentlichen Beitrag zum Cybersicherheitsökosystem der Union geleistet. Ihre Rolle bei der Unterstützung nationaler Bemühungen und der Bereitstellung von Erkenntnissen zu neu auftretenden Bedrohungen war von entscheidender Bedeutung. Interessenträger aus dem Privatsektor kritisierten jedoch, dass die Unterstützung zielgerichteter gestaltet werden müsse, was darauf hindeutet, dass die Einbeziehung der Interessenträger und die Zusammenarbeit mit der Industrie verbessert werden müssen. Durch eine strategische Neubewertung des Ressourcenmanagements könnte sich die ENISA besser auf die sich wandelnden Herausforderungen im Bereich der Cybersicherheit ausrichten und für verschiedene Interessenträger von größerem Nutzen sein. Mit dem ECCF sollten harmonisierte Zertifizierungsverfahren eingeführt werden, allerdings gab es aufgrund von langwierigen Verfahren und Fragmentierung Herausforderungen bei der Umsetzung. Der Mehrwert des ECCF war begrenzt, da die Ziele nicht erreicht wurden und es an Effizienz mangelte. Trotz dieser Herausforderungen hat der ECCF die Harmonisierung zwischen den Mitgliedstaaten verbessert und bessere Kooperationsmöglichkeiten geschaffen, insbesondere durch

die Einrichtung von Foren für die Zusammenarbeit von Interessenträgern wie der Europäischen Gruppe für die Cybersicherheitszertifizierung (ECCG).

- **Konsultation der Interessenträger**

Zwischen 2023 und 2025 wurden die Interessenträger mehrfach konsultiert, und zwar sowohl zur Bewertung des Rechtsakts zur Cybersicherheit als auch zur Überarbeitung dieses Rechtsakts:

– **2023** wurden 65 Befragungen durchgeführt (52 davon konzentrierten sich vor allem auf die ENISA und 13 hauptsächlich auf den ECCF); zudem gab es eine Erhebung, zu der 209 Antworten eingingen (wovon sich 70 auf den ECCF bezogen), eine öffentliche Konsultation wurde abgeschlossen, und es wurden zwei Workshops mit 26 bzw. 70 Teilnehmern zur SWOT-Analyse (Analyse der Stärken, Schwächen, Chancen und Risiken) und zu Empfehlungen abgehalten. Diese Tätigkeiten zielten konkret darauf ab, die Ansichten der Interessenträger einzuholen, um die Wirkung, Wirksamkeit und Effizienz der ENISA zu bewerten. Der Abschlussbericht der im Auftrag der Kommission von PwC, Intellera Consulting und PPMI durchgeführten Studie zur Unterstützung der Bewertung der Agentur der Europäischen Union für Cybersicherheit (ENISA) und des europäischen Rahmens für die Cybersicherheitszertifizierung (2024) wurde im Dezember 2024 fertiggestellt.

– **2025** veröffentlichte die Kommission eine Aufforderung zur Stellungnahme. Insbesondere wurden die Interessenträger aufgefordert, schriftliche Beiträge, wie Positionspapiere, technische Berichte oder Stellungnahmen, zu konkreten Reformvorschlägen, einzureichen. Insgesamt gingen 184 Einzelbeiträge aus einem breiten Spektrum von Interessengruppen ein, darunter Industrieverbände, Cybersicherheitsunternehmen, KMU, akademische Einrichtungen und gemeinnützige Organisationen.

– **Zwischen April und Juni 2025** führte die Kommission eine öffentliche Konsultation im Rahmen der Überarbeitung des Rechtsakts zur Cybersicherheit durch; es gingen 193 Antworten ein. Die Konsultation umfasste 38 teils geschlossene, teils offene Fragen zum Mandat der ENISA, zum ECCF, zur Sicherheit der IKT-Lieferketten und zur Vereinfachung.

– **Gezielte Konsultation (Befragungen):** Mit ausgewählten Interessenträgern wurde eine Reihe teilstrukturierter Befragungen durchgeführt. Dazu gehörten Vertreter der ENISA sowie nationale Behörden, die nationale Meldeplattformen entwickelt haben oder verwalten. Im Mittelpunkt der Befragungen standen die Rolle und die Kapazitäten der ENISA, die operative Funktionsweise des ECCF, praktische Herausforderungen bei der Angleichung der Zertifizierungsverfahren auf nationaler und Unionsebene, der Meldeaufwand und Hindernisse bei der Umsetzung. Aus diesen Befragungen konnten qualitative Erkenntnisse gewonnen werden, die in die Auswertung der Ergebnisse der öffentlichen Konsultation einflossen und zur Verfeinerung der politischen Optionen beitrugen.

– Hinzu kamen **Konsultationen von Vertretern der Mitgliedstaaten im Rahmen der Arbeitsgruppe des Rates[19] und in bilateralen Gesprächen,** in denen die Mitgliedstaaten ihre Ansichten zur Überarbeitung des Rechtsakts zur Cybersicherheit vorbringen konnten.

– **Gezielte Konsultation (ECCF-Gruppen – ECCG, Gruppe der Interessenträger für die Cybersicherheitszertifizierung (SCCG)):** Die Kommission legte in ihrer Eigenschaft als

[19] Horizontale Gruppe „Fragen des Cyberraums“ des Rates.

Vorsitzende beider Gruppen in den Sitzungen der ECCG am 12. März und 3. Juli 2025 und in der SCCG-Sitzung am 17. März 2025 den Sachstand in Bezug auf die Überarbeitung des Rechtsakts zur Cybersicherheit dar. Darüber hinaus wurden mithilfe von Fragebögen zusätzliche fachliche Stellungnahmen von Mitgliedern der ECCG eingeholt.

Die Konsultation konzentrierte sich auf fünf Kernbereiche, die für das künftige Funktionieren und die Kohärenz des Cybersicherheitsrahmens der Union von zentraler Bedeutung sind:

- **das Mandat und die operative Rolle der ENISA**, einschließlich der Unterstützung der Mitgliedstaaten und der Bereitstellung von Sachkenntnis im Bereich neu aufkommender Technologien;
- **die Wirksamkeit des europäischen Rahmens für die Cybersicherheitszertifizierung**, einschließlich Governance- und Entwicklungsprozessen;
- **die Komplexität und Fragmentierung der Anforderungen an die Cybersicherheit** mit einem Schwerpunkt auf dem Meldeaufwand und möglichen Vereinfachungen;
- **die Verhältnismäßigkeit der Anforderungen für KMU** und Möglichkeiten, bei der Rechtsbefolgung zu differenzieren, und
- **gesellschaftliche und wirtschaftliche Auswirkungen** harmonisierter Cybersicherheitsvorschriften, einschließlich der Auswirkungen auf Verbraucher, Rechte, Innovation und Wettbewerbsfähigkeit.
- **Folgenabschätzung**

In die Überarbeitung des Rechtsakts zur Cybersicherheit wie auch den Vorschlag für eine Richtlinie mit gezielten Änderungen der NIS-2-Richtlinie flossen die Ergebnisse einer Folgenabschätzung ein (siehe nachstehende Zusammenfassung). Der Ausschuss für Regulierungskontrolle gab eine befürwortende Stellungnahme mit Vorbehalten zu dem erneut vorgelegten Entwurf des Berichts über die Folgenabschätzung im Zusammenhang mit der Überarbeitung des Rechtsakts zur Cybersicherheit[20] ab. Die Folgenabschätzung wurde entsprechend angepasst, um den Empfehlungen und Anmerkungen des Ausschusses für Regulierungskontrolle Rechnung zu tragen.

Der endgültige Politikvorschlag weicht nicht von den in der Folgenabschätzung bewerteten Optionen ab.

Die Kommission prüfte im Hinblick auf die zu erreichenden spezifischen Ziele Optionen in vier Interventionsbereichen: 1. das Mandat der ENISA (auch Teil des derzeitigen Rechtsakts zur Cybersicherheit); 2. den ECCF (auch Teil des derzeitigen Rechtsakts zur Cybersicherheit); 3. gezielte Änderungen der NIS-2-Richtlinie mit dem Ziel der Vereinfachung, wobei dieser Punkt aber auch mit dem Mandat der ENISA und dem ECCF verknüpft ist, und 4. die Sicherheit der IKT-Lieferketten, die sowohl für das NIS-2-Ökosystem als auch für den ECCF von Bedeutung ist. Die einzelnen Bündel an Optionen stellen einen jeweils eigenen Interventionsbereich dar, sind aber gleichzeitig miteinander verknüpft und füreinander relevant.

[20] Verordnung (EU) 2019/881 (http://data.europa.eu/eli/reg/2019/881/oj).

Optionen zur Auflösung der Diskrepanz zwischen dem politischen Rahmen der Union für die Cybersicherheit und den Bedürfnissen der Interessenträger in einer zunehmend feindseligen Umgebung

Option A.1: *Präzisierung des Mandats der ENISA und Festlegung von Prioritäten* – Mit dieser Option würde ein klarer, stabiler Rahmen für die Aufgaben der ENISA geschaffen, indem die in anderen Rechtsvorschriften enthaltenen Aufgaben in diesen Rechtsakt aufgenommen würden.

Option A.2: *Reform des Mandats der ENISA* – Mit dieser Option würde der Rechtsakt zur Cybersicherheit aufgehoben und ersetzt und dadurch das Mandat der Agentur neu gefasst.

Option A.3: *Reform des Mandats der ENISA mit besonderem Augenmerk auf operative Unterstützung* – Diese Option würde auf Option A.2 aufbauen. Darüber hinaus würde die ENISA Fähigkeiten entwickeln, um Einrichtungen gemäß der NIS-2-Richtlinie auf Ersuchen eines Mitgliedstaats bei der Reaktion auf Cybersicherheitsvorfälle und der Wiederherstellung danach unmittelbar zu unterstützen.

Optionen für den ECCF

Option B.1: *Klarstellung des Umfangs, der Elemente und Ziele des ECCF und Einführung eines Mechanismus für die Systempflege* – Mit dieser Option würde ein neuer, von der ENISA umzusetzender Mechanismus für die Pflege der Systeme nach ihrer Annahme geschaffen.

Option B.2: *Reform des ECCF durch Überarbeitung der Verfahren und Ausweitung des Umfangs, um die Einhaltung von Vorschriften zu erleichtern* – Mit dieser Option würde der Rechtsakt zur Cybersicherheit aufgehoben und durch eine neue Verordnung ersetzt. Zusätzlich zu Option B.1 würden die Verfahren im Zusammenhang mit der Inauftraggabe, Entwicklung und Annahme von Systemen überarbeitet, um die Rechenschaftspflicht und Effizienz zu verbessern.

Option B.3: *Reform des ECCF gemäß Option B.2 plus Einführung einer obligatorischen Zertifizierung für Cyberabwehr* – Diese Option würde auf Option B.2 aufbauen, aber auch darauf abzielen, die Wirkung des Rahmens weiter zu erhöhen, indem eine obligatorische Zertifizierung für wesentliche Einrichtungen eingeführt würde, bei der spezifische Risikoszenarien berücksichtigt würden, anstatt sich ausschließlich auf die freiwillige Zertifizierung von Einrichtungen zu verlassen.

Optionen zur Vereinfachung

Option C.1: *Verfolgung eines Soft-Law-Ansatzes und der Anwendung nicht legislativer Instrumente, einschließlich der Nutzung bestehender Befugnisübertragungen (Erlass von Durchführungsrechtsakten gemäß Artikel 21 Absatz 5 und Artikel 23 Absatz 11 der NIS-2-Richtlinie)* – Diese Option beinhaltet den Erlass von Durchführungsrechtsakten auf der Grundlage bestehender Befugnisübertragungen im Rahmen der NIS-2-Richtlinie, um für mehr Harmonisierung bei den Risikomanagementmaßnahmen im Bereich der Cybersicherheit, bei den Schwellenwerten für die Meldung von Sicherheitsvorfällen sowie bei der Art der Informationen, der Formate und des Meldeverfahrens zu sorgen. Ferner ist die Annahme einer Reihe von Leitlinien vorgesehen, um die Rechtssicherheit und die harmonisierte Umsetzung zu verbessern.

Option C.2: *Gezieltes Tätigwerden – weitere Vereinfachung der Einhaltung des einschlägigen Rechtsrahmens der Union für die Cybersicherheit* – Diese Option beinhaltet ein begrenztes Tätigwerden durch Änderungen des Rechtsakts zur Cybersicherheit und der NIS-2-Richtlinie mit dem Ziel, bestimmte Aspekte des Cybersicherheitsrahmens zu vereinfachen,

einschließlich Anpassungen des Umfangs, einer größtmöglichen Harmonisierung bei Durchführungsrechtsakten, des Nachweises der Rechtsbefolgung durch Zertifizierung und der Annahme einer Reihe von Leitlinien, wie unter Option C.1 vorgesehen.

Option C.3: *Harmonisierung der in den Unionsvorschriften enthaltenen Maßnahmen im Bereich der Cybersicherheit* – Diese Option würde auf Option C.2 aufbauen; zudem würden alle in sektoralen Rechtsvorschriften enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und alle Befugnisübertragungen im Zusammenhang mit solchen Maßnahmen gestrichen. Stattdessen würde das Ökosystem der NIS-2-Richtlinie geändert, um gestraffte Anforderungen für alle Arten von Einrichtungen festzulegen und so für mehr Harmonisierung zu sorgen.

Optionen für die Sicherheit der IKT-Lieferketten

Option D.1: Verfolgung eines *Soft-Law-Ansatzes zur Reaktion auf Cybersicherheitsrisiken in den IKT-Lieferketten* – Bei dieser Option würden auf EU-Ebene keine Regulierungsmaßnahmen ergriffen. Stattdessen würde die Kommission die Zahl der koordinierten Risikobewertungen und der freiwilligen Instrumentarien erhöhen.

Option D.2: *Ad-hoc-Regulierungsmaßnahmen zur Kodifizierung des 5G-Instrumentariums* – Mit dieser Option würden die Maßnahmen zum 5G-Instrumentarium kodifiziert. Dadurch würden die Mitgliedstaaten verpflichtet, dafür zu sorgen, dass in wichtigen Assets des Netzes keine Komponenten von Hochrisikoanbietern verwendet werden.

Option D.3: *Umfassender horizontaler Rahmen, um den Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen* – Mit dieser Option würde ein horizontaler, technologie- und branchenneutraler Regelungsrahmen geschaffen, um nicht technischen Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen.

Nach eingehender Analyse hat sich folgende Kombination von Optionen als bevorzugtes Maßnahmenpaket erwiesen: Option A.2 (Reform des Mandats der ENISA); Option B.2 (Reform des ECCF durch Überarbeitung der Verfahren und Ausweitung des Umfangs, um die Einhaltung von Vorschriften zu erleichtern); Option C.2 (gezieltes Tätigwerden – weitere Vereinfachung der Einhaltung des einschlägigen Rechtsrahmens der Union für die Cybersicherheit) und Option D.3 (umfassender horizontaler Rahmen, um den Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen).

Diese Kombination bietet eine ausgewogene Antwort auf die ermittelten politischen Herausforderungen und verbessert die Wirksamkeit, Effizienz und Kohärenz in der gesamten Union erheblich.

Die Umsetzung der vorgeschlagenen bevorzugten Option für den Regelungsrahmen wird Kosten verursachen, sowohl für die ENISA, die neue Aufgaben erfüllen muss (schätzungsweise bis zu 161,3 Mio. EUR über einen Zeitraum von fünf Jahren), als auch für die Behörden in der gesamten Union, die Kosten für die Beaufsichtigung tragen müssen (schätzungsweise bis zu 80 Mio. EUR über einen Zeitraum von fünf Jahren unter Berücksichtigung der relevanten Kosteneinsparungen). Was die Unternehmen betrifft, so könnte die schrittweise Aussonderung bestimmter Hochrisikoausrüstungen über einen Zeitraum von fünf Jahren zu jährlichen Kosten von 3,4 bis 4,3 Mrd. EUR für Mobilfunknetzbetreiber führen, während die Investitionen in vertrauenswürdige Anbieter auf bis zu 2 Mrd. EUR pro Jahr steigen könnten.

Gleichzeitig dürften gestraffte und reduzierte Rechtsbefolgungspflichten über einen Zeitraum von fünf Jahren zu Kosteneinsparungen von bis zu 15,3 Mrd. EUR für Unternehmen führen. Darüber hinaus würden eine Verbesserung der allgemeinen Cyberabwehr und der technologischen Souveränität der Union sowie die Förderung von Innovation und Wettbewerbsfähigkeit erhebliche Vorteile für die breite Öffentlichkeit, Behörden und Unternehmen mit sich bringen. Dies dürfte die anfänglich entstehenden Ausgaben langfristig weitgehend ausgleichen.

Durch weniger Marktfragmentierung und harmonisierte regulatorische Anforderungen sorgen die bevorzugten Optionen für fairere Wettbewerbsbedingungen in der gesamten Union und bieten den Unternehmen klarere Perspektiven für die Einhaltung von Vorschriften und Innovationen.

Die bevorzugten Optionen würden durch klare Leitlinien und integrierte Systeme auch zur Vereinfachung beitragen und den Verwaltungsaufwand verringern. Die Optionen entsprechen dem One-in-one-out-Grundsatz, da sichergestellt wird, dass neue Verpflichtungen durch den Wegfall von Verpflichtungen an anderer Stelle ausgeglichen werden.

- **Effizienz der Rechtsetzung und Vereinfachung**

Die Überarbeitung des Rechtsakts zur Cybersicherheit trägt durch die ausgewählten politischen Optionen A.2, B.2, C.2 und D.3 erheblich zur Verbesserung der Klarheit, zur Beseitigung von Ineffizienzen und zur Angleichung von Verfahren über die verschiedenen Rechtsrahmen hinweg bei. Konkret wird in Option A.2 eine vollständige Reform des Mandats der ENISA vorgeschlagen, um die Umsetzung der Politik und die operative Zusammenarbeit zwischen den Mitgliedstaaten wirksam zu unterstützen. Diese Konsolidierung wird auch dazu beitragen, fragmentierte Praktiken zu beseitigen, die Koordinierung zu verbessern und gleichzeitig die Befolgungs- und Betriebskosten langfristig zu senken. Option B.2, die die Aufhebung des derzeitigen Rechtsakts zur Cybersicherheit und die Einführung eines reformierten ECCF umfasst, erhöht die Effizienz durch die Überarbeitung des Governance-Modells und die Unterstützung berechenbarerer, kohärenterer und flexiblerer Zertifizierungsverfahren. Dadurch können Systeme schneller angenommen und besser an bereichsübergreifende Rechtsvorschriften angeglichen, die regulatorische Fragmentierung reduziert und Belastungen sowohl für öffentliche als auch für private Interessenträger verringert werden. Mit der Option C.2 werden die Befolgungskosten für Einrichtungen gesenkt, die den einschlägigen Rechtsvorschriften der Union im Bereich der Cybersicherheit unterliegen, und zwar durch Änderungen des Umfangs und durch die Ermöglichung organisatorischer Systeme für die Cybersicherheitszertifizierung für Einrichtungen, die in den Anwendungsbereich der NIS-2-Richtlinie und anderer Rechtsakte fallen. Dieser Ansatz wird die regulatorischen Verpflichtungen für Einrichtungen, die mehreren Anforderungen unterliegen, erheblich vereinfachen und eine wirksamere Nutzung der Ressourcen durch die nationalen Behörden gewährleisten. Mit Option D.3 wird ein harmonisierter Rahmen für die Bewältigung nicht technischer Risiken geschaffen, die sich auf die IKT-Lieferketten auswirken, wodurch die derzeit inkohärenten Ansätze in den Mitgliedstaaten einheitlicher gestaltet werden. Zusammengenommen stellen diese Optionen eine erhebliche Vereinfachung und Modernisierung des Rechtsrahmens der Union für die Cybersicherheit dar, was vollständig den REFIT-Grundsätzen der Klarheit, Effizienz und Bereitschaft für den digitalen Wandel entspricht.

Der Vorschlag steht im Einklang mit dem „Digitalcheck“, da die Konzentration auf straffere digitale Prozesse zeigt, dass sich die Union für einen Zuerst-digital-Ansatz einsetzt, der einen schnelleren und zuverlässigeren Datenaustausch und eine schnellere und zuverlässigere

Entscheidungsfindung gewährleistet. Option D.3 könnte auch große Auswirkungen auf die Digitalisierung haben, da Komponenten ersetzt würden, die von Einrichtungen stammen, die in Drittländern, für die Cybersicherheitsbedenken bestehen, niedergelassen sind oder von Einrichtungen in solchen Drittländern kontrolliert werden (Hochrisikoanbieter).

- **Grundrechte**

Dieser Gesetzgebungsvorschlag wurde auf der Grundlage seines Potenzials zur Stärkung oder Gefährdung der Grundrechte und zur Förderung von Gleichheit und Vertrauen bewertet, wobei ein besonderer Schwerpunkt auf den gesellschaftlichen Auswirkungen und Rechten lag, einschließlich des Schutzes der Privatsphäre, des Datenschutzes und der Möglichkeit des Einzelnen, seine Rechte zu verstehen, auszuüben und durchzusetzen.

Die Ausweitung des Mandats der ENISA wird zu mehr Cyberresilienz in der Wirtschaft und der Gesellschaft insgesamt beitragen und zu einem besseren Schutz der Privatsphäre und der personenbezogenen Daten der Menschen führen. Der Vorschlag wird auch die Aus- und Weiterbildung im Bereich der Cybersicherheit unterstützen, da darin die Rolle der ENISA bei der Entwicklung von Kompetenzen für Fachkräfte im Bereich der Cybersicherheit präzisiert wird.

Darüber hinaus wird der ECCF das Vertrauen der breiten Öffentlichkeit und der Unternehmen in der Union in zertifizierte IKT-Lösungen stärken, die im täglichen Leben hilfreich sind. Die Einführung zusätzlicher Systeme würde diese Wirkung noch verstärken.

Der Vorschlag trägt zum Vertrauen der Menschen bei, indem er Einrichtungen in kritischen Sektoren Anreize bietet, eine Cybersicherheitszertifizierung anzustreben, wodurch sie ihr hohes Maß an Cybersicherheit öffentlich nachweisen. Darüber hinaus würde die harmonisierte Berichterstattung über Ransomware-Vorfälle und das Ergreifen von Maßnahmen für den Übergang zur Post-Quanten-Kryptografie das Vertrauen der Öffentlichkeit in den Schutz sensibler Daten in kritischen Sektoren stärken.

Die Bestimmungen über die Sicherheit der Lieferketten werden sich in gewissem Maße auf den Schutz der Grundrechte auswirken, denn sie begrenzen Einflussnahmen aus dem Ausland. Aktivitäten wie Spionage und Überwachung untergraben die Grundrechte der Bürgerinnen und Bürger erheblich. Dieser horizontale Rahmen hätte das Potenzial, das Vertrauen, die Sicherheit und den Schutz der Privatsphäre bei verschiedenen Technologien und digitalen Lösungen zu verbessern.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Die Mittelausstattung der EU-Cybersicherheitsagentur (ENISA), die zu erheblich mehr Sicherheit der EU beitragen wird, wurde mit 341 Mio. EUR für sieben Jahre bzw. einem durchschnittlichen Jahresbudget von 49 Mio. EUR veranschlagt (Prognose für 2028 bis 2034). Dies entspricht einer Aufstockung der Mittel der Agentur um 81,5 % gegenüber 2025. Der mit der vorgeschlagenen Initiative generierte Nutzen wird entsprechend der Analyse in der Folgenabschätzung erheblich sein und Kosteneinsparungen von bis zu 14,6 Mrd. EUR für Unternehmen bringen. Das Ausmaß der potenziellen Kosteneinsparungen im Zusammenhang mit einer generell besseren Bereitschaft der Union zur Abwehr von Cybersicherheitsvorfällen lässt sich naturgemäß schwer quantifizieren, es wird jedoch davon ausgegangen, dass die Kosteneinsparungen durch eine schnellere Reaktion auf Cybersicherheitsvorfälle und eine geringere Ausbreitung solcher Vorfälle über einen Zeitraum von fünf Jahren zwischen 3,7 Mrd. EUR und 4,4 Mrd. EUR liegen könnten. Im Zusammenhang mit künftigen politischen Initiativen wird die Kommission die allgemeine Verteilung der Ressourcen für die

und innerhalb der Organe, Einrichtungen, Agenturen und sonstigen Stellen der EU im Bereich der Cybersicherheit prüfen, um Wissen und Sachkenntnis zu nutzen und Synergien zu ermitteln und auszubauen.
Die zur Stärkung der Agentur vorgeschlagenen zusätzlichen Ressourcen belaufen sich auf 118 VZÄ und zusätzliche Mittel für operative Kosten, aus denen nicht nur laufende Beitragsvereinbarungen zwischen der ENISA und der Kommission, wie z. B. für die Pflege der einheitlichen Meldeplattform, finanziert werden, sondern auch die VZÄ, die mit dem Betrieb und der Verwaltung der EU-Cybersicherheitsreserve befasst sind, sowie wichtige Initiativen der Kommission wie die Entwicklung der zentralen Anlaufstelle im Rahmen des Digital-Omnibus-Vorschlags. Weitere operative Kosten stehen im Zusammenhang mit dem Programm zur koordinierten Offenlegung von Schwachstellen, der Erhebung und Analyse von Erkenntnissen über Cybersicherheitsbedrohungen, der sicheren Kommunikation und dem Aufbau der Cybersicherheitsreife für die ENISA. Die operativen Kosten für die Pflege der europäischen Systeme für die Cybersicherheitszertifizierung, die Erteilung von Befugnissen zur Ausstellung von Bescheinigungen im Bereich der Cybersicherheitskompetenzen und die Dienstleistungen im Bereich von Testinstrumenten werden ebenfalls aus diesen Mitteln finanziert, sie werden jedoch auch teilweise durch Mechanismen zur Eigenfinanzierung in Form von Gebühren getragen.

Ein wichtiger Aspekt des Vorschlags ist die Einführung von Gebührenmechanismen, die neben anderen politischen Zielen auch zu einem nachhaltigen Finanzkreislauf innerhalb der Agentur beitragen werden. Der überarbeitete Rechtsakt zur Cybersicherheit sieht drei Arten von Gebühren vor, die in den Haushalt der ENISA fließen werden, nämlich Gebühren für die Erteilung von Befugnissen für Kompetenzbescheinigungen, Gebühren für die Dienstleistungen im Bereich von Testinstrumenten und Gebühren für die Unterstützung bei der Pflege der europäischen Systeme für die Cybersicherheitszertifizierung. Das erwartete Plus für den EU-Haushalt wird für den Siebenjahreszeitraum 2028-2034 auf rund 18,5 Mio. EUR geschätzt.

Der Haushaltsantrag der Kommission enthält 50 zusätzliche VZÄ-Stellen. Dieses Personal soll den Rahmen für die Lieferketten umsetzen und u. a. Aufgaben im Zusammenhang mit der Ausarbeitung von Durchführungsrechtsakten für die Gebührenmechanismen, die Pflege von Zertifizierungssystemen, die Normung und die Unterstützung der operativen Zusammenarbeit übernehmen. Die Kosten, die der Kommission durch die Umsetzung des Rahmens für die Lieferketten entstehen, dürften wohl insbesondere von der Zahl der von der Kommission durchgeführten Bewertungen der Eigentums- und Kontrollverhältnisse abhängen. Die hierbei erzielten Ergebnisse werden jedoch erheblich zu Einsparungen für die Mitgliedstaaten bei der Beaufsichtigung der Umsetzung von Abhilfemaßnahmen und Verpflichtungen beitragen, die den NIS-2-Einrichtungen durch den Rahmen auferlegt werden. Die Mitgliedstaaten werden die Ergebnisse der Bewertungen der Eigentums- und Kontrollverhältnisse direkt nutzen können, anstatt jeweils einzeln Ressourcen für denselben Bewertungsbedarf aufzuwenden.

Ausführlichere Informationen finden sich im Finanzbogen zum Cyberpaket.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Überwachungs-, Bewertungs- und Berichterstattungsmodalitäten**

Die Kommission wird die Anwendung der vorgeschlagenen Verordnung überwachen und dem Europäischen Parlament und dem Rat alle fünf Jahre einen Bericht über ihre Bewertung

vorlegen. Diese Berichte werden veröffentlicht und geben detailliert Auskunft über die tatsächliche Anwendung und Durchsetzung der vorgeschlagenen Verordnung.

- **Erläuternde Dokumente (bei Richtlinien)**

Entfällt, da es sich bei dem Vorschlag um eine Verordnung handelt.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Der Vorschlag präzisiert die Rolle der ENISA und überträgt ihr konkrete Aufgaben zur Unterstützung von Interessenträgern, allen voran der Mitgliedstaaten, insbesondere in Bezug auf die Unterstützung bei der Umsetzung der Politik und der Rechtsvorschriften der Union, die operative Zusammenarbeit, den Kapazitätsaufbau, die Cybersicherheitszertifizierung und Normung sowie die Weiterbildung der Fachkräfte im Bereich der Cybersicherheit und deren unionsweite Mobilität. Der Vorschlag zielt ferner darauf ab, den europäischen Rahmen für die Cybersicherheitszertifizierung (ECCF) wirksamer und effizienter zu gestalten, um das Cybersicherheitsniveau in der Union zu verbessern und die Kunden in die Lage zu versetzen, bei der Beschaffung von IKT-Produkten, -Diensten und -Prozessen sowie von verwalteten Sicherheitsdiensten im gesamten Binnenmarkt fundierte Entscheidungen zu treffen. Darüber hinaus zielt dieser Vorschlag in Verbindung mit dem Vorschlag für eine Richtlinie mit gezielten Änderungen der NIS-2-Richtlinie darauf ab, die Einhaltung der Anforderungen an die Cybersicherheit zu vereinfachen und Ressourcen freizusetzen, um die operative Abwehrbereitschaft im Bereich der Cybersicherheit von Einrichtungen in den kritischen Sektoren der Union zu stärken. Schließlich trägt der Vorschlag der Notwendigkeit Rechnung, die Wirtschaft und die IKT-Lieferketten der Union widerstandsfähiger zu machen, um ihre eigene Sicherheit und Wettbewerbsfähigkeit zu fördern. Einzelheiten werden nachstehend erläutert.

TITEL I: ALLGEMEINE BESTIMMUNGEN

Titel I der vorgeschlagenen Verordnung enthält die allgemeinen Bestimmungen: Gegenstand (Artikel 1) und Begriffsbestimmungen (Artikel 2), einschließlich Verweisen auf die einschlägigen Begriffsbestimmungen aus anderen Unionsinstrumenten, wie der Richtlinie (EU) 2022/2555[21] (NIS-2-Richtlinie), der Verordnung (EG) Nr. 765/2008[22] und der Verordnung (EU) Nr. 1025/2012[23].

TITEL II: ENISA (AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT)

Titel II der vorgeschlagenen Verordnung enthält die wichtigsten Bestimmungen betreffend die ENISA.

Kapitel I enthält den Auftrag (Artikel 3) und die Ziele (Artikel 4) der ENISA.

In Kapitel II werden die Aufgaben der Agentur in drei Abschnitten dargelegt.

Abschnitt 1 enthält Bestimmungen zu den Aufgaben im Zusammenhang mit der Unterstützung der Umsetzung der Unionspolitik und des Unionsrechts. Darin ist festgelegt, welche Einrichtungen und Organisationen Unterstützung in welcher Form erhalten sollen

21 http://data.europa.eu/eli/dir/2022/2555/oj.
22 http://data.europa.eu/eli/reg/2008/765/oj.
23 http://data.europa.eu/eli/reg/2012/1025/oj.

(Artikel 5). In Artikel 6 sind die Zuständigkeiten der Agentur für den Kapazitätsaufbau geregelt, einschließlich der Bereitstellung von Wissen und Sachkenntnis für die Mitgliedstaaten in Bezug auf die Prävention und Bewältigung von Cyberbedrohungen, die Aktualisierung der Cybersicherheitsstrategien und den Ausbau der Fachkräftebasis im Bereich der Cybersicherheit. Die ENISA wird die Mitgliedstaaten auch bei ihren Sensibilisierungsmaßnahmen unterstützen (Artikel 7), die wichtigsten Markttrends im Bereich der Cybersicherheit analysieren und technische Empfehlungen und Analysen verbreiten (Artikel 8). Außerdem wird sie zur internationalen Zusammenarbeit in Fragen der Cybersicherheit gemäß Artikel 9 beitragen und diese fördern.

Abschnitt 2 enthält die Aufgaben der ENISA in Bezug auf die operative Zusammenarbeit mit den Mitgliedstaaten, den Einrichtungen der Union und dem CERT-EU, dem Netzwerk der Computer-Notfallteams (CSIRTs), dem EU-CyCLONe und anderen Interessenträgern, einschließlich der Herausgabe von Leitlinien und der Einführung sicherer Kommunikationsinstrumente (Artikel 10). Die ENISA wird auch dazu beitragen, die Lageerfassung bei Cyberbedrohungen und -vorfällen zu verbessern, indem sie (unter anderem) eine oder mehrere Ablage(n) von Erkenntnissen über Cyberbedrohungen entwickelt, Analysen durchführt und Frühwarnungen ausgibt (Artikel 11). Die Vorschriften für solche Frühwarnungen (Inhalt, zeitlicher Ablauf, Dienst) sind in Artikel 12 festgelegt. Um wesentliche und wichtige Einrichtungen bei der Vorbereitung und Reaktion auf Ransomware-Vorfälle sowie bei der Wiederherstellung danach zu unterstützen, betreibt die ENISA die EU-Cybersicherheitsreserve gemäß Artikel 13 und arbeitet gegebenenfalls mit Europol und den CSIRTs oder anderen zuständigen Behörden zusammen. Artikel 14 enthält Bestimmungen über die Rolle der ENISA bei Cybersicherheitsübungen auf Unionsebene, einschließlich der Erstellung eines jährlichen fortlaufenden Programms für Cybersicherheitsübungen auf Unionsebene. Zusätzlich zu diesen Aufgaben sollte die ENISA Instrumente und Plattformen bereitstellen, insbesondere die gemäß Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 eingerichtete einheitliche Meldeplattform (Artikel 15). Schließlich muss die Agentur einen gemeinsamen Schwachstellenmanagementdienst der Union entwickeln und Schwachstellenmanagementdienste bereitstellen (Artikel 16).

In Abschnitt 3 über die Cybersicherheitszertifizierung und Normung sind die diesbezüglichen Aufgaben der Agentur festgelegt. Artikel 17 beschreibt die Rolle der ENISA bei der Entwicklung und Umsetzung des ECCF, einschließlich ihrer führenden Rolle bei der Ausarbeitung von Systemen und der Gewährleistung ihrer Pflege und ihres Kapazitätsaufbaus, während in Artikel 18 dargelegt ist, wie die ENISA an der Ausarbeitung technischer Spezifikationen mitwirken und zu Normungstätigkeiten auf europäischer und internationaler Ebene, auch im Bereich der kryptografischen Algorithmen, beitragen sollte.

In Abschnitt 4 sind die Aufgaben der Agentur im Zusammenhang mit der Einrichtung der Akademie für Cybersicherheitskompetenzen geregelt. Artikel 19 enthält Bestimmungen über die Rolle der ENISA in Bezug auf den europäischen Rahmen für Cybersicherheitskompetenzen (ECSF), während ihre Aufgaben in Bezug auf die Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen in Artikel 20 festgelegt sind. Die Anforderungen an befugte Bescheinigungsanbieter sind in Artikel 21 und die Vorgaben für die Bearbeitung von Anträgen in Artikel 22 enthalten. Die ENISA muss öffentliche Informationen im Zusammenhang mit dem ECSF und Bescheinigungen individueller Cybersicherheitskompetenzen bereitstellen (Artikel 23).

Kapitel III betrifft die Organisation der ENISA. Die Verwaltungs- und Leitungsstruktur der Agentur umfasst auch einen stellvertretenden Exekutivdirektor (Artikel 24). Abschnitt 1 enthält Bestimmungen über den Verwaltungsrat, seine Zusammensetzung, seinen Vorsitz, seine Sitzungen, Aufgaben und Abstimmungsregeln (Artikel 25 bis 29). Der Exekutivrat unterstützt den Verwaltungsrat gemäß Abschnitt 2 Artikel 30. Abschnitt 3 enthält Vorschriften über die Ernennung und Abberufung des Exekutivdirektors und die Verlängerung seiner Amtszeit (Artikel 31) sowie Vorschriften über die Aufgaben und Zuständigkeiten des Exekutivdirektors (Artikel 32). Der Verwaltungsrat kann beschließen, einen stellvertretenden Exekutivdirektor einzusetzen, der den Exekutivdirektor unterstützt (Abschnitt 4 Artikel 33 und 34). Der Verwaltungsrat muss die ENISA-Beratungsgruppe einsetzen, die die ENISA gemäß Artikel 35 berät. Abschnitt 6 enthält Vorschriften über die Einsetzung und Zusammensetzung der Beschwerdekammer (Artikel 36) und über deren Mitglieder (Artikel 37). In Artikel 38 sind die Umstände, unter denen die Mitglieder der Beschwerdekammer nicht am Beschwerdeverfahren teilnehmen dürfen, und die Gründe für die Ablehnung eines Mitglieds der Beschwerdekammer festgelegt. Die Beschwerdekammer kann mit Beschwerden gegen Entscheidungen der ENISA oder wegen Untätigkeit der ENISA befasst werden (Artikel 39). Artikel 40 umfasst Bestimmungen über die Personen, die eine Beschwerde einlegen können, die Frist und die Form der Beschwerde. Die Artikel 41 bis 43 enthalten Vorschriften über die Abhilfe, die Prüfung von Entscheidungen über Beschwerden und Klagen beim Gerichtshof. Artikel 44 schließlich regelt das Verfahren im Zusammenhang mit dem einheitlichen Programmplanungsdokument.

Kapitel IV betrifft die Aufstellung und die Gliederung des Haushaltsplans der Agentur sowie die Vorschriften für dessen Darstellung und Ausführung (Artikel 45 bis 55). Es enthält auch Bestimmungen, durch die die Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen erleichtert werden soll (Artikel 51).

Kapitel V betrifft das Personal der Agentur. Es enthält allgemeine Bestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen für andere Beschäftigte sowie Vorschriften über Vorrechte und Befreiungen (Artikel 56 und 57). Es werden Bestimmungen eingeführt, mit denen die Mitgliedstaaten verpflichtet werden, Verbindungsbeamte als abgeordnete nationale Sachverständige für die ENISA zu benennen; zudem ist deren Rolle in der Agentur geregelt (Artikel 58). Das Kapitel enthält auch Bestimmungen über den Einsatz abgeordneter nationaler Sachverständiger und sonstigen Personals, das nicht von der Agentur selbst beschäftigt wird (Artikel 59).

Kapitel VI schließlich enthält die allgemeinen Bestimmungen für die Agentur. Darin sind ihre Rechtsform (Artikel 60) und ihr Sitz festgelegt (Artikel 61) und Bestimmungen über das Sitzabkommen und die Arbeitsbedingungen der Agentur sowie über die Verwaltungskontrolle durch den Bürgerbeauftragten enthalten (Artikel 62 und 63). Das Kapitel umfasst Bestimmungen bezüglich Haftung, Sprachenregelung und den Schutz personenbezogener Daten (Artikel 64 bis 66) sowie Sicherheitsvorschriften für den Schutz von nicht als Verschlusssache eingestuften sensiblen Informationen und von Verschlusssachen (Artikel 67). Es regelt die Zusammenarbeit mit den Einrichtungen der Union und nationalen Behörden (Artikel 68) sowie mit anderen Interessenträgern (Artikel 69). In dem Kapitel sind auch Vorschriften für die Zusammenarbeit der Agentur mit Drittländern und internationalen Organisationen (Artikel 70) festgelegt.

TITEL III: EUROPÄISCHER RAHMEN FÜR DIE CYBERSICHERHEITSZERTIFIZIERUNG

Mit Titel III der vorgeschlagenen Verordnung wird der ECCF eingerichtet.

In Kapitel I werden die Ziele, der Umfang und die Verfahren des Rahmens vorgestellt. Zu den Zielen (Artikel 71) gehören die Stärkung der Cybersicherheit in der gesamten Union und die Erleichterung eines harmonisierten Ansatzes für die Zertifizierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen. Im Rahmen des ECCF sollte auch die Zertifizierung genutzt werden, um die Einhaltung der geltenden Rechtsvorschriften der Union im Wege der Konformitätsvermutung zu vereinfachen und so den Aufwand für die Unternehmen zu verringern (Artikel 78). In Kapitel I sind Verfahrensaspekte geregelt, beginnend mit Konsultationen zu strategischen europäischen Prioritäten für die Cybersicherheitszertifizierung und öffentlichen Informationen im Zusammenhang mit der Entwicklung des Systems durch die Kommission sowie der Einrichtung einer neuen europäischen Versammlung für die Cybersicherheitszertifizierung (Artikel 72). Auf detaillierte Beauftragung durch die Kommission (Artikel 73) wird erwartet, dass die ENISA innerhalb von 12 Monaten ein mögliches System bereitstellt. Artikel 74 enthält weitere Fristen für die Vorlage der Stellungnahme der ECCG und die Bereitstellung des Systems zur Annahme durch die Kommission. Mit Artikel 75 wird ein klarer Mechanismus für die Pflege bestehender Systeme eingeführt, der eine Überprüfung solcher Systeme nach sich ziehen könnte (Artikel 76). Die Überprüfung eines Systems könnte sich ferner auf eine regelmäßige Bewertung der Wirksamkeit des Systems und seiner Auswirkungen auf den Binnenmarkt stützen. Artikel 77 enthält die Grundlagen für die Ausarbeitung technischer Spezifikationen durch die ENISA zur Unterstützung bei der Entwicklung und Pflege europäischer Systeme für die Cybersicherheitszertifizierung. Bei der Annahme oder Überprüfung eines Systems kann die Kommission auf solche technischen Spezifikationen Bezug nehmen (Artikel 74). Die verschiedenen Verfahren gewährleisten die Transparenz und Qualität der Durchführung, indem in verschiedenen Phasen der Planung, Entwicklung, Annahme und Pflege von Zertifizierungssystemen Sachverständige und andere Interessenträger hinzugezogen werden. Gemäß Artikel 79 betreibt die ENISA eine eigene Website zu europäischen Systemen für die Cybersicherheitszertifizierung, auf der Informationen über angenommene Systeme sowie europäische Cybersicherheitszertifikate und im Rahmen dieser Systeme ausgestellte EU-Konformitätserklärungen bereitgestellt werden sollten.

Kapitel II umfasst allgemeine Vorschriften für den Inhalt der europäischen Systeme für die Cybersicherheitszertifizierung.

Artikel 80 enthält eine Liste von Sicherheitszielen, nach denen ein System von der ENISA auszugestalten ist, und gewährleistet die Angleichung an die einschlägigen Rechtsvorschriften im Bereich der Cybersicherheit. Jedes europäische System für die Cybersicherheitszertifizierung kann die in Artikel 81 genannten Elemente enthalten. Diese Elemente müssen mit den Rechtsvorschriften der Union vereinbar sein und können unter Verwendung von Musterbestimmungen für alle Systeme harmonisiert werden. Beide Bestimmungen bieten die notwendige Flexibilität zur Anpassung an verschiedene Arten von Systemen. In weiteren Bestimmungen sind die Vertrauenswürdigkeitsstufen (Artikel 82) und die Selbstbewertung der Konformität (Artikel 83) geregelt. Das Kapitel enthält außerdem eine Liste ergänzender Informationen (Artikel 84), die der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen bereitstellen muss.

In Kapitel III schließlich sind die Vorschriften für die Governance des ECCF festgelegt, wobei dieses Kapitel in drei Abschnitte unterteilt ist.

Abschnitt 1 betrifft Vorschriften für die Ausstellung europäischer Cybersicherheitszertifikate, auch solcher der Vertrauenswürdigkeitsstufe „hoch“ (Artikel 85). Darüber hinaus enthält dieser Abschnitt Vorschriften für die Harmonisierung der europäischen Systeme für die Cybersicherheitszertifizierung mit den nationalen Cybersicherheitszertifizierungssystemen und Cybersicherheitszertifikaten (Artikel 86) und sieht die Möglichkeit der internationalen Anerkennung europäischer Cybersicherheitszertifikate auf der Grundlage des Grundsatzes der Gleichwertigkeit vor (Artikel 87). In diesem Abschnitt geht es außerdem um die Rolle der nationalen Behörden für die Cybersicherheitszertifizierung und die für sie geltenden Vorschriften (Artikel 88) und um Vorschriften für einen Mechanismus der gegenseitigen Begutachtung unter diesen Behörden, um gleichwertige Normen in der gesamten Union zu gewährleisten (Artikel 89), sowie Vorschriften für die Zusammenarbeit zwischen diesen Behörden im Rahmen der ECGG (Artikel 90).

Abschnitt 2 enthält: i) harmonisierte Vorschriften für die Akkreditierung und Zulassung von Konformitätsbewertungsstellen (Artikel 91 und 92); ii) Vorschriften für die Notifizierung, einschließlich einer Befugnisübertragung zur Gewährleistung einer weiteren Angleichung an das einschlägige Unionsrecht und den neuen Rechtsrahmen (Artikel 93), und iii) ein Anfechtungsverfahren (Artikel 94), mit dem sichergestellt wird, dass die Anforderungen an Konformitätsbewertungsstellen eingehalten werden.

Abschnitt 3 regelt schließlich die Rechte und Rechtsbehelfe gegen Zertifizierungsentscheidungen (Artikel 96) und verpflichtet die Mitgliedstaaten, verhältnismäßige Sanktionen für Verstöße gegen Vorschriften festzulegen und durchzusetzen.

TITEL IV

In Kapitel I Artikel 98 ist der Umfang des Rahmens für vertrauenswürdige IKT-Lieferketten festgelegt. Der Rahmen wird sich mit nicht technischen Risiken in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren gemäß der Richtlinie (EU) 2022/2555 befassen. Im Rahmen des Mechanismus werden wichtige IKT-Assets in kritischen IKT-Lieferketten ermittelt und geeignete und verhältnismäßige Risikominderungsmaßnahmen für die in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen festgelegt. Der Rahmen wird sich auf auf Unionsebene koordinierte Sicherheitsrisikobewertungen stützen, um die die Kommission oder mindestens drei Mitgliedstaaten ersuchen. In Artikel 99 ist festgelegt, wie diese Risikobewertungen durchgeführt werden und dass auch Risikominderungsmaßnahmen festgelegt werden sollten. Diese Risikobewertungen sollten innerhalb von sechs Monaten nach dem Ersuchen abgeschlossen werden. Auf Ersuchen der Kommission kann die NIS-Kooperationsgruppe einer kürzeren Frist zustimmen. Der Rahmen sieht ein Notfallverfahren vor, wenn ein sofortiges Eingreifen gerechtfertigt ist, um das reibungslose Funktionieren des Binnenmarkts zu erhalten, und wenn die Kommission hinreichenden Grund zu der Annahme hat, dass in Bezug auf kritische IKT-Lieferketten eine erhebliche Cyberbedrohung für die Sicherheit der Union besteht. In diesem Fall konsultiert die Kommission die Mitgliedstaaten bezüglich der Notwendigkeit, eine oder mehrere Risikominderungsmaßnahmen zu ergreifen, und führt eine Risikobewertung durch. Wenn sich infolge der Risikobewertung gemäß Artikel 99 oder anhand anderer Quellen, wie einer öffentlichen Erklärung im Namen der Union oder eines Mitgliedstaats, zeigt, dass von einem Drittland schwerwiegende, strukturelle nicht technische Risiken für die IKT-Lieferketten ausgehen, muss die Kommission gemäß Artikel 100 die von diesem Drittland ausgehende Bedrohung unter Berücksichtigung der in Artikel 100 aufgeführten Elemente überprüfen. Gelangt die Kommission zu dem Schluss, dass von einem Drittland schwerwiegende, strukturelle nicht technische Risiken für die IKT-Lieferketten

ausgehen, sieht Artikel 100 ein Verfahren vor, nach dem die Kommission ein solches Drittland als Land benennt, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen. Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen und das gemäß diesem Artikel benannt wurde, niedergelassen sind oder die von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert werden, dürfen eine Reihe von in dem genannten Artikel aufgeführten Tätigkeiten nicht durchführen. Artikel 101 sieht einen allgemeinen Sicherheitsmechanismus für IKT-Lieferketten vor, bei dem die Kommission nach Abschluss der Sicherheitsrisikobewertung durch die NIS-Kooperationsgruppe oder die Kommission gemäß Artikel 99 die in den Artikeln 102 und 103 aufgeführten Maßnahmen ergreifen kann.

Die Kommission kann im Wege von Durchführungsrechtsakten wichtige IKT-Assets ermitteln, die zur Herstellung von Produkten und zur Erbringung von Dienstleistungen durch die in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen eingesetzt werden. Artikel 102 enthält weitere Elemente, die bei der Ermittlung wichtiger IKT-Assets zu berücksichtigen sind. In Artikel 103 sind mögliche Risikominderungsmaßnahmen in der IKT-Lieferkette festgelegt. Die Kommission kann im Wege von Durchführungsrechtsakten beschließen, dass Einrichtungen, die in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren tätig sind, spezifischen Risikominderungsmaßnahmen unterliegen müssen; diese werden in dem genannten Artikel näher ausgeführt.

Nachdem die Kommission eine Bewertung der Niederlassung, des Eigentums und der Kontrolle vorgenommen hat, erstellt sie im Wege von Durchführungsrechtsakten Listen von Hochrisikoanbietern, für die die mit Durchführungsrechtsakten gemäß Artikel 103 Absatz 1 oder Absatz 7 erlassenen Verbote oder das Verbot gemäß Artikel 110 Absatz 1 relevant sind. Hierzu sollte sie die betreffenden Anbieter und die zuständigen Behörden konsultieren (Artikel 104).

Eine Einrichtung, die in einem Drittland, für das Cybersicherheitsbedenken bestehen und das gemäß Artikel 100 benannt wurde, niedergelassen ist oder von Einrichtungen aus einem solchen Drittland kontrolliert wird, kann beantragen, IKT-Komponenten für wichtige IKT-Assets der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art von Einrichtungen bereitstellen und sich an öffentlichen Ausschreibungen im Zusammenhang mit der Bereitstellung solcher IKT-Komponenten beteiligen zu dürfen. In Artikel 105 ist festgelegt, was der Antrag enthalten sollte und wie eine solche Ausnahmegenehmigung erteilt werden kann. Artikel 106 enthält die Verteidigungsrechte betroffener Einrichtungen. Die Kommission führt ein öffentlich zugängliches Register der Beschlüsse über Ausnahmegenehmigungen (Artikel 107). Die Artikel 108 und 109 enthalten die Bestimmungen betreffend die Vertraulichkeit und die Gebühren im Zusammenhang mit Ausnahmegenehmigungen.

Kapitel II sieht die Anwendung des Rahmens für vertrauenswürdige IKT-Lieferketten auf mobile, feste und satellitengestützte elektronische Kommunikationsnetze zur Angleichung an die vorgeschlagene Verordnung über digitale Netze vor.

Die wichtigen IKT-Assets für mobile, feste und satellitengestützte elektronische Kommunikationsnetze sind in Anhang II festgelegt. Der Übergangszeitraum für die schrittweise Entfernung der von Hochrisikoanbietern bereitgestellten IKT-Komponenten für wichtige IKT-Assets elektronischer Mobilfunk-Kommunikationsnetze darf 36 Monate ab dem Inkrafttreten dieser Verordnung nicht überschreiten. Die Übergangszeiträume für feste und

satellitengestützte elektronische Kommunikationsnetze werden von der Kommission im Wege von Durchführungsrechtsakten festgelegt. Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zur Änderung bestimmter wichtiger IKT-Assets und von Übergangszeiträumen, auch für künftige Generationen von Mobilfunknetzen, zu erlassen (Artikel 110). In Artikel 111 ist festgelegt, dass Anbieter mobiler, fester und satellitengestützter elektronischer Kommunikationsnetze IKT-Komponenten von Hochrisikoanbietern in keiner Form nutzen, installieren oder integrieren dürfen und dafür keine allgemeine oder individuelle Zulassung erteilt werden darf.

Zuständige Behörden, Beaufsichtigung und Durchsetzung, rechtliche Zuständigkeit, Verteidigungsrechte (Kapitel III)

Kapitel III enthält Vorschriften über die zuständigen Behörden, die Beaufsichtigung und Durchsetzung sowie die rechtliche Zuständigkeit.

In den Artikeln 112 bis 114 sind die Befugnisse, Mittel und Zuständigkeiten der Mitgliedstaaten bei der Durchführung und Durchsetzung der Bestimmungen des Titels IV geregelt. Die Mitgliedstaaten müssen eine oder mehrere zuständige Behörden benennen, die der Kommission notifizieren sind. Artikel 113 sieht vor, dass die Kommission ein Netz für die Zusammenarbeit der zuständigen Behörden der Mitgliedstaaten und der Kommission einrichtet, um die Einhaltung der Vorschriften zu erleichtern, während in Artikel 114 die Aufsichts- und Durchsetzungsmaßnahmen festgelegt sind, die die zuständigen Behörden ergreifen dürfen. Die Sanktionen bei Verstößen gegen die Bestimmungen des Titels IV sind in Artikel 115 geregelt. In Artikel 116 ist festgelegt, dass sich die Mitgliedstaaten gegenseitig unterstützen können, wenn Einrichtungen grenzübergreifend tätig sind oder wenn sich ihre wichtigen IKT-Assets in mehreren Mitgliedstaaten befinden. Artikel 117 enthält die Vorschriften über die rechtliche Zuständigkeit und die Territorialität.

TITEL VI: SCHLUSSBESTIMMUNGEN

Titel VI der vorgeschlagenen Verordnung enthält die Schlussbestimmungen, in denen die Vorschriften für den Erlass von Durchführungsrechtsakten und delegierten Rechtsakten, das Bewertungsverfahren für die vorgeschlagene Verordnung sowie die Aufhebung und Rechtsnachfolge der Verordnung (EU) 2019/881 dargelegt sind. Zudem ist das Datum des Inkrafttretens der vorgeschlagenen Verordnung angegeben.

2026/0011 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses[24],

nach Stellungnahme des Ausschusses der Regionen[25],

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Seit der Annahme der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[26] hat es erhebliche geopolitische, technologische und politische Veränderungen gegeben. Cybersicherheitsvorfälle, unabhängig davon, ob sie durch Systemausfälle, menschliches Versagen, böswillige Handlungen oder Naturphänomene verursacht werden, haben zugenommen, und Cyberangriffe sind ausgefeilter geworden und betreffen wesentliche Einrichtungen, Unternehmen und die breite Öffentlichkeit. Cyberkriminalität hat sich rasant verbreitet, wobei Ransomware-Vorfälle im Mittelpunkt stehen. Immer häufiger kommt es zu Vorfällen in Lieferketten, die von Kriminellen, die finanziell Profit schlagen wollen, oder von staatlichen Akteuren zum Zweck der Unterbrechung der Lieferketten, der Spionage, Desinformation oder Kriegsführung verursacht werden. Vorfälle, die auf böswillige Cyberaktivitäten und Systemausfälle zurückzuführen sind, sind oft Teil einer umfassenderen hybriden Strategie, sodass sie sich ausbreiten, wesentliche Dienste stören, das Vertrauen in Institutionen untergraben und die Abwehrbereitschaft der Gesellschaft sowie die Verteidigungsbereitschaft der Union beeinträchtigen. Solche

---

24 ABl. C , , S. .

25 ABl. C , , S. .

26 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

Vorfälle haben gezeigt, wie schädlich sie für die Wirtschaftstätigkeit, die Finanzstabilität und das Leben der Menschen sein können. Gleichzeitig stellen die Schwachstellen kritischer ziviler Infrastrukturen und Systeme ein Risiko für die Verteidigungsfähigkeiten dar, die teilweise auf diese Infrastrukturen und Systeme angewiesen sind.

(2) Parallel dazu wirken sich neu aufkommende Technologien wie künstliche Intelligenz und Quanteninformatik negativ auf die Cybersicherheit und die Cyberabwehr aus. Sie verändern die Verteidigungsinstrumente und die Taktiken der Gegner, stellen Bedrohungen für die Cybersicherheit und die Cyberabwehr dar und eröffnen gleichzeitig Chancen für technologischen Fortschritt. Zwar können diese Technologien durch eine verbesserte Erkennung von Bedrohungen oder eine automatisierte Reaktion auf Sicherheitsvorfälle zur Cybersicherheit beitragen, doch sie bieten auch zusätzliche Angriffsfläche für Organisationen, sind potenzielle Ziele für Manipulationen und können langfristig die Wirkung von Sicherheitsmaßnahmen wie Verschlüsselung untergraben.

(3) Um diesen Entwicklungen Rechnung zu tragen, hat die Union ihre rechtlichen und politischen Instrumente ausgeweitet. Durch die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[27], ergänzt durch die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates[28] über die physische Sicherheit, wird die Cybersicherheit kritischer Infrastrukturen verstärkt. Mit der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates[29] wird die Cybersicherheit von Produkten mit digitalen Elementen verbessert. Mit der Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates[30] werden unionsweite Reaktionsfähigkeiten aufgebaut, und durch die Empfehlung des Rates vom 6. Juni 2025 für einen EU-Konzeptentwurf für das Cyberkrisenmanagement[31] (im Folgenden „Empfehlung zum Cyberkonzeptentwurf“) wird die Zusammenarbeit bei der Krisenbewältigung auf Unionsebene unterstützt. Das Instrumentarium für die 5G-Cybersicherheit[32] ist ein erster Schritt hin zu einem unionsweit koordinierten Ansatz zur Sicherung der 5G-Netze. Die Mitteilung der Kommission über die Akademie für

---

27 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

28 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (ABl. L 333 vom 27.12.2022, S. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

29 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

30 Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung) (ABl. L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

31 ABl. C, C/2025/3445, 20.6.2025, ELI: http://data.europa.eu/eli/C/2025/3445/oj.

32 Cybersicherheit von 5G-Netzen – EU-Instrumentarium für Risikominderungsmaßnahmen, NIS-Kooperationsgruppe, 1/2020, abrufbar unter: https://digital-strategy.ec.europa.eu/de/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

Cybersicherheitskompetenzen[33] behandelt die wachsende Herausforderung des Fachkräftemangels im Bereich der Cybersicherheit. Darüber hinaus wurde der Cybersicherheitsrahmen durch sektorspezifische Rechtsvorschriften erweitert, insbesondere die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates[34] für den Finanzsektor, die Delegierte Verordnung (EU) 2024/1366 der Kommission[35] für den Teilsektor Strom, die Delegierte Verordnung (EU) 2022/1645 der Kommission[36] und die Durchführungsverordnung (EU) 2023/203 der Kommission[37] (Teil-IS) sowie einschlägige Vorschriften über die Luftsicherheit gemäß der Verordnung (EU) 2019/1583 der Kommission[38] für den Teilsektor Luftverkehr und andere Strategiepapiere wie die Mitteilung der Kommission über einen EU-Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern[39]. Die Einrichtungen der Union werden auch durch die Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates[40]

---

33 Mitteilung der Kommission an das Europäische Parlament und den Rat – Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU („Akademie für Cybersicherheitskompetenzen"), COM(2023) 207 final, 18. April 2023.

34 Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (ABl. L 333 vom 27.12.2022, S. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

35 Delegierte Verordnung (EU) 2024/1366 der Kommission vom 11. März 2024 zur Ergänzung der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates durch Festlegung eines Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse (ABl. L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

36 Delegierte Verordnung (EU) 2022/1645 der Kommission vom 14. Juli 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission (ABl. L 248 vom 26.9.2022, S. 18, ELI: http://data.europa.eu/eli/reg_del/2022/1645/oj).

37 Durchführungsverordnung (EU) 2023/203 der Kommission vom 27. Oktober 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates hinsichtlich der Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 der Kommission, die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie für zuständige Behörden, die unter die Verordnungen (EU) Nr. 748/2012, (EU) Nr. 1321/2014, (EU) Nr. 965/2012, (EU) Nr. 1178/2011, (EU) 2015/340 und (EU) Nr. 139/2014 der Kommission und die Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission fallen, sowie zur Änderung der Verordnungen (EU) Nr. 1178/2011, (EU) Nr. 748/2012, (EU) Nr. 965/2012, (EU) Nr. 139/2014, (EU) Nr. 1321/2014, (EU) 2015/340 der Kommission und der Durchführungsverordnungen (EU) 2017/373 und (EU) 2021/664 der Kommission (ABl. L 31 vom 2.2.2023, S. 1, ELI: http://data.europa.eu/eli/reg_impl/2023/203/oj).

38 Durchführungsverordnung (EU) 2019/1583 der Kommission vom 25. September 2019 zur Änderung der Verordnung (EU) 2015/1998 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Luftsicherheit in Bezug auf Cybersicherheitsmaßnahmen (ABl. L 246 vom 26.9.2019, S. 15, ELI: http://data.europa.eu/eli/reg_impl/2019/1583/oj).

39 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Europäischer Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern, COM(2025) 10 final, 15. Januar 2025.

40 Verordnung (EU, Euratom) 2023/2841 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union (ABl. L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

gestärkt, in der Maßnahmen festgelegt sind, mit denen innerhalb der Organe, Einrichtungen und sonstigen Stellen der Union ein hohes gemeinsames Cybersicherheitsniveau erreicht werden soll. Durch diesen erweiterten Rechtsrahmen für die Cybersicherheit wurden die Aufgaben der ENISA weiter präzisiert.

(4) In diesem Zusammenhang und entsprechend ProtectEU – eine Europäische Strategie für die innere Sicherheit[41] und der Strategie für eine Union der Krisenvorsorge[42] braucht es zur Gewährleistung der Krisenvorsorge, Sicherheit und Resilienz der Gesellschaft und der Wirtschaft der Union eine enge europäische Abstimmung, Vertrauen und Informationsaustausch zwischen Interessenträgern, robuste Rahmen zur Gewährleistung der Sicherheit von IKT-Produkten, -Diensten und -Prozessen sowie von verwalteten Sicherheitsdiensten und den Ausbau und die Verbesserung der Fachkräftebasis im Bereich der Cybersicherheit. Darüber hinaus gilt es, die IKT-Lieferketten zu stärken, indem sichergestellt wird, dass Europa die technologische Souveränität über wichtige Assets hat, was wiederum die Resilienz der Union erhöhen und den Bemühungen im Bereich der Cyberabwehr zugutekommen würde. Darüber hinaus werden in der Mitteilung über die Stärkung der wirtschaftlichen Sicherheit der EU[43] als vorrangige Ziele genannt, dass der Zugang zu sensiblen Informationen und Daten, die die wirtschaftliche Sicherheit der EU untergraben könnten, verhindert und Störungen kritischer Infrastrukturen der EU, die sich auf die Wirtschaft der EU auswirken, verhindert und abgemildert werden müssen. In der Mitteilung wird anerkannt, welche wesentliche Rolle wirksame Cybersicherheitsmaßnahmen dabei spielen.

(5) Cybersicherheitsvorfälle großen Ausmaßes, die kritische Infrastrukturen, digitale Dienste oder wesentliche gesellschaftliche Funktionen beeinträchtigen, können Auswirkungen auf die Bevölkerung haben, die koordinierte Katastrophenschutz- und Krisenmanagementmaßnahmen auf Unionsebene erfordern. Im Einklang mit dem gefahrenübergreifenden Ansatz der Europäischen Strategie für eine Union der Krisenvorsorge und dem Beschluss Nr. 1313/2013/EU über das Katastrophenschutzverfahren der Union sollten die Vorkehrungen für die Lageerfassung, die Reaktion auf Sicherheitsvorfälle und Übungen im Rahmen dieser Verordnung in das Krisenmanagement der Union einfließen, insbesondere über das Zentrum für die Koordination von Notfallmaßnahmen (ERCC).

(6) Dieser Vorschlag steht im Einklang mit und wird ergänzt durch den [Vorschlag für eine Richtlinie zur Ergänzung der [Überarbeitung der Verordnung (EU) 2019/881] und der Änderungsrichtlinie (EU) 2022/2555 betreffend die Vereinfachung der Durchführung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union] sowie mit dem [Vorschlag für eine Verordnung zur Vereinfachung des digitalen Rechtsrahmens (Digital-Omnibus-Verordnung)[44]], der die ENISA verpflichtet, eine zentrale Anlaufstelle für die Meldung von Sicherheitsvorfällen

---

41 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: ProtectEU – eine Europäische Strategie für die innere Sicherheit, COM(2025) 148 final, 1. April 2025.

42 Gemeinsame Mitteilung an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über die Europäische Strategie für eine Union der Krisenvorsorge, JOIN(2025) 130 final.

43 Gemeinsame Mitteilung an das Europäische Parlament und den Rat über die Stärkung der wirtschaftlichen Sicherheit der EU, JOIN(2025) 977 final.

44 COM(2025) 837 final.

einzurichten, über die Einrichtungen ihren Pflichten zur Meldung von Sicherheitsvorfällen gemäß mehreren Rechtsakten gleichzeitig nachkommen können.

(7) Mit der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates[45] wurde die ENISA errichtet, um innerhalb der Union zu einer hohen und effektiven Netz- und Informationssicherheit und zur Herausbildung einer Kultur der Netz- und Informationssicherheit beizutragen, die Bürgern, Verbrauchern, Unternehmen und öffentlichen Verwaltungen zugutekommt. Das Mandat der ENISA wurde dreimal verlängert, bevor ihr mit der Verordnung (EU) 2019/881 ein ständiges Mandat erteilt wurde. Um dem Bedarf, der sich aufgrund der veränderten Bedrohungslage und der technologischen Entwicklungen ergibt, besser gerecht zu werden, insbesondere im Hinblick auf die operative Zusammenarbeit und den gestiegenen Bedarf an Cybersicherheitsfachkräften, sollte das Mandat der ENISA weiter gestärkt werden. Im Interesse der Rechtssicherheit sollte die Verordnung (EU) 2019/881 ersetzt werden.

(8) Angesichts einer sich wandelnden Bedrohungslage, in der Cybersicherheitsvorfälle immer größere Auswirkungen haben, ist es wichtiger denn je, das Vertrauen von Einzelpersonen, Behörden und Unternehmen in die tägliche Nutzung von Technologien zu stärken. Dies kann durch eine verstärkte unionsweite Zertifizierung im Rahmen des ECCF erleichtert werden, für die über nationale Märkte und Sektoren hinaus einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden. Der neue Rahmen sollte die wichtigsten horizontalen Anforderungen an europäische Systeme für die Cybersicherheitszertifizierung festlegen und es ermöglichen, dass europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen in allen Mitgliedstaaten anerkannt und verwendet werden. Hierzu sollten ein Verfahren und ein Governance-Rahmen geschaffen werden, die die rechtzeitige und vorhersehbare Entwicklung und Pflege europäischer Systeme für die Cybersicherheitszertifizierung ermöglichen. Die europäischen Systeme für die Cybersicherheitszertifizierung sollten in allen Mitgliedstaaten einheitlich angewandt werden, um eine harmonisierte Umsetzung der Cybersicherheitsanforderungen zu gewährleisten, gleiche Wettbewerbsbedingungen zu schaffen und ein „Zertifizierungsshopping“ aufgrund unterschiedlicher Anforderungsniveaus in den einzelnen Mitgliedstaaten zu verhindern. Die ENISA sollte eine Schlüsselrolle dabei spielen, die Systeme durch technische Spezifikationen weiterzuentwickeln und sicherzustellen, dass diese Systeme technisch auf dem neuesten Stand bleiben. Um den Markterfordernissen wirksam gerecht zu werden, sollte der Rahmen darüber hinaus die Möglichkeit der Zertifizierung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit vorsehen, die an Einrichtungen gerichtet sind, und die Einhaltung anderer geltender Rechtsvorschriften der Union im Bereich der Cybersicherheit erleichtern. Die Angleichung an bestehende Unionsvorschriften wie die Verordnung (EU) 2024/2847 und die Richtlinie (EU) 2022/2555 ist von entscheidender Bedeutung, damit die europäischen Systeme für die Cybersicherheitszertifizierung dazu beitragen, den Befolgungsaufwand für Unternehmen zu verringern, ihre Attraktivität zu erhöhen und die Cyberresilienz der Union zu stärken.

(9) Die ENISA sollte den Auftrag haben, die Mitgliedstaaten und die Einrichtungen der Union dabei zu unterstützen, in der Union ein hohes Maß an Cybersicherheit, Resilienz und Vertrauen zu erreichen. Zu diesem Zweck sollte die ENISA als

[45] Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1, ELI: http://data.europa.eu/eli/reg/2004/460/oj).

Bezugspunkt für Beratung und Sachkenntnis im Bereich der Cybersicherheit dienen, und ihre Arbeit sollte sich in erster Linie auf vier Schlüsselbereiche der Cybersicherheit auf Unionsebene konzentrieren. Erstens sollte die ENISA die Mitgliedstaaten bei der kohärenten Umsetzung der Politik und der Rechtsvorschriften der Union im Bereich der Cybersicherheit unterstützen und den Mitgliedstaaten durch Maßnahmen zum Kapazitätsaufbau dabei helfen, ihre Kapazitäten bei der Abwehrbereitschaft, Resilienz und Reaktion kontinuierlich zu verbessern. Zweitens sollte die ENISA zur operativen Zusammenarbeit auf Unionsebene und zwischen den Mitgliedstaaten sowie zu einer besseren gemeinsamen Lageerfassung in Bezug auf Cyberbedrohungen und -vorfälle zwischen den Mitgliedstaaten und den Einrichtungen der Union beitragen. Der dritte Schlüsselbereich sollte die Zertifizierung und Standardisierung der Cybersicherheit sein, während der vierte Schlüsselbereich die Einrichtung der Akademie für Cybersicherheitskompetenzen betrifft, die dazu beitragen sollte, die europäische Fachkräftebasis im Bereich der Cybersicherheit zu stärken und diesen Fachkräften Kompetenzen zu vermitteln, die in alle Mitgliedstaaten übertragbar sind.

(10) Die Verordnung (EU, Euratom) 2023/2841 zur Festlegung von Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in den Organen, Einrichtungen und sonstigen Stellen der Union enthält das Mandat des CERT-EU, mit dem er als Cybersicherheitsdienst für die Organe, Einrichtungen und sonstigen Stellen der Union eingerichtet wird, um zur Sicherheit der nicht für Verschlusssachen genutzten IKT-Umgebung von Einrichtungen der Union beizutragen, indem er diese in Cybersicherheitsangelegenheiten berät, bei der Prävention, Erkennung, Handhabung, Eindämmung und Bewältigung von Sicherheitsvorfällen und der Wiederherstellung danach unterstützt und als zentrale Stelle für den Austausch von Informationen zur Cybersicherheit und die Koordinierung der Reaktion auf Sicherheitsvorfälle fungiert. Darüber hinaus hat der CERT-EU die Aufgabe, den Einrichtungen der Union relevante Cybersicherheitsdienste anzubieten. Im Rahmen ihres Auftrags sollte die ENISA auch die Einrichtungen der Union unterstützen. Dies sollte insbesondere durch eine strukturierte Zusammenarbeit mit dem CERT-EU bei Kapazitätsaufbau, operativer Zusammenarbeit und langfristigen strategischen Analysen von Cyberbedrohungen erfolgen. Gegebenenfalls kann die ENISA die strukturierte Zusammenarbeit mit dem CERT-EU für von ihr bereitgestellte Cybersicherheitsdienste oder Unterstützungsleistungen, die für die Einrichtungen der Union einen Mehrwert darstellen können, in koordinierter Weise nutzen, um für Synergien mit den Bemühungen des CERT-EU zu sorgen.

(11) Eine der Hauptaufgaben der ENISA sollte darin bestehen, die Mitgliedstaaten bei der einheitlichen Umsetzung der Politik und des Rechts der Union im Bereich der Cybersicherheit zu unterstützen, insbesondere bezüglich der Richtlinie (EU) 2022/2555, der Verordnung (EU) 2024/2847 und der Verordnung (EU) 2025/38. Für eine kohärente und wirksame Umsetzung des Besitzstands der Union im Bereich der Cybersicherheit sollte die ENISA technische Leitlinien und Berichte herausgeben, Beratungsleistungen und bewährte Verfahren bereitstellen und den diesbezüglichen Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtern. Darüber hinaus bewertet die ENISA den Stand der Cybersicherheit in der Union und nimmt zu diesem Zweck einen Bericht gemäß Artikel 18 der Richtlinie (EU) 2022/2555 an. Die ENISA sollte zudem in der Lage sein, auf Ersuchen der Mitgliedstaaten und gegebenenfalls von Einrichtungen der Union um Rat und Hilfestellung zu Angelegenheiten, die durch das Mandat der ENISA abgedeckt sind, zu reagieren.

(12) Um die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor sowie innerhalb des privaten Sektors anzukurbeln, insbesondere um den Schutz kritischer Infrastrukturen zu fördern, sollte die ENISA den Informationsaustausch innerhalb von und zwischen Sektoren, insbesondere den in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren, sowie Informationen über Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) 2024/2847 fallen, unterstützen. Diese Unterstützung kann in Form von bewährten Verfahren und Leitlinien zu verfügbaren Instrumenten und Verfahren sowie in Form von Leitlinien für den Umgang mit Regulierungsfragen im Zusammenhang mit dem Informationsaustausch erfolgen, z. B. durch die Erleichterung der Einrichtung sektorspezifischer Informationsaustausch- und -analysezentren.

(13) Im Hinblick auf die Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs sollte die ENISA zur Arbeit der mit der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe (im Folgenden „NIS-Kooperationsgruppe“) beitragen, indem sie insbesondere Sachkenntnis und Beratung bereitstellt und den Austausch bewährter Verfahren, unter anderem im Zusammenhang mit grenzübergreifenden Abhängigkeiten, in Bezug auf Risiken und Sicherheitsvorfälle erleichtert. Die ENISA sollte auch zur Arbeit der durch die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[46] eingesetzten europäischen Kooperationsgruppe für die digitale Identität, der Europäischen Gruppe für die Cybersicherheitszertifizierung und der durch die Verordnung (EU) 2024/2847 eingesetzten Gruppe zur administrativen Zusammenarbeit (ADCO) beitragen.

(14) Der öffentliche Kern des offenen Internets, d. h. seine wichtigsten Protokolle und Infrastrukturen, die ein globales öffentliches Gut sind, stellt die wesentlichen Funktionen des Internets als Ganzes bereit und bildet die Grundlage für dessen normalen Betrieb. Im Rahmen ihres Mandats sollte die ENISA die Sicherheit und Resilienz des öffentlichen Kerns des offenen Internets und die Stabilität seines Funktionierens unterstützen, unter anderem durch die sichere Einführung und den sicheren Einsatz wichtiger Protokolle (insbesondere Domain-Namen-System, Border-Gateway-Protokoll und Version 6 des Internet-Protokolls) und den Betrieb des Domain-Namen-Systems (wie den Betrieb aller Domänen der obersten Ebene), indem sie bewährte Verfahren, Leitlinien und Zusammenarbeit im Einklang mit den bestehenden globalen Multi-Stakeholder-Regelungen für die Internet-Governance und den jeweiligen Aufgaben und Zuständigkeiten der einschlägigen internationalen technischen und operativen Einrichtungen fördert.

(15) Die ENISA dient als Bezugspunkt für Beratung und Sachkenntnis im Bereich der Cybersicherheit. Daher sollte die ENISA die Kommission auf deren Ersuchen durch Sachkenntnis, technische Beratung, Informationen, Analysen, einschließlich Durchführbarkeitsstudien, Stellungnahmen und vorbereitende Arbeiten, zu spezifischen Fragen im Bereich der Cybersicherheit unterstützen, um zur Politikgestaltung der Kommission beizutragen und es der Kommission zu erleichtern, die Umsetzung der Rechtsvorschriften der Union im Bereich der Cybersicherheit zu überwachen.

---

[46] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(16) Ebenso sollte die ENISA aufgrund ihrer Sachkenntnis die Mitgliedstaaten in ihrem Bemühen um den Auf- und Ausbau der Fähigkeiten und der Bereitschaft zur Verhütung, Erkennung und Bewältigung von Cyberbedrohungen und von Sicherheitsvorfällen im Zusammenhang mit der Netz- und Informationssicherheit unterstützen. So sollte die ENISA den Auf- und Ausbau der in der Richtlinie (EU) 2022/2555 vorgesehenen Computer-Notfallteams (CSIRTs) unterstützen, damit diese ein unionsweit hohes Maß an Ausgereiftheit erreichen.

(17) Die ENISA hat die Mitgliedstaaten bei der Entwicklung und Umsetzung von Leitlinien für ihre nationalen Cybersicherheitsstrategien unterstützt und sollte sie weiterhin unterstützen, um dazu beizutragen, dass alle Mitgliedstaaten Cybersicherheitsstrategien annehmen und umsetzen. Die ENISA sollte die Verbreitung solcher Strategien über die interaktive Karte der nationalen Cybersicherheitsstrategien fördern und die Fortschritte bei ihrer Umsetzung weiter verfolgen, unter anderem durch Unterstützung bei der Entwicklung diesbezüglicher wesentlicher Leistungsindikatoren.

(18) Mit der Verordnung (EU, Euratom) 2023/2841 wurde der Interinstitutionelle Cybersicherheitsbeirat beauftragt, die Einrichtungen der Union dabei zu unterstützen, ihre jeweilige Cybersicherheitslage zu verbessern, und der CERT-EU wurde beauftragt, zur Sicherheit der nicht für Verschlusssachen genutzten IKT-Umgebung aller Einrichtungen der Union beizutragen. Die ENISA sollte auf der Grundlage ihrer Erfahrungen im Bereich der Cybersicherheit den Interinstitutionellen Cybersicherheitsbeirat und den CERT-EU bei der Erfüllung ihrer Aufgaben gemäß der Verordnung (EU, Euratom) 2023/2841 unterstützen, unter anderem durch Beiträge zur Analyse von Cyberbedrohungen, zur Lageerfassung, zu Cybersicherheitsübungen, zur Koordinierung der Reaktion auf Sicherheitsvorfälle und zum Austausch von Know-how und bewährten Verfahren.

(19) Auf der Grundlage der Sachkenntnis der ENISA und zur Ergänzung der Kapazitäten nationaler Behörden und Unionsbehörden sollte die ENISA Schulungen auf der Grundlage des europäischen Rahmens für Cybersicherheitskompetenzen (ECSF) abhalten, um insbesondere die wirksame Umsetzung politischer Maßnahmen, die operative Zusammenarbeit und die Sensibilisierung zu unterstützen.

(20) Um für Synergien mit dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC) und dem gemäß der Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates[47] eingerichteten Netzwerk nationaler Koordinierungszentren zu sorgen, sollte die ENISA diese durch die Weitergabe von Informationen über aktuelle und neu auftretende Risiken und Cyberbedrohungen unterstützen, auch über Risiken und Bedrohungen im Zusammenhang mit Informations- und Kommunikationstechnologien.

(21) In der Strategie für die Krisenvorsorge wird betont, dass der Erwerb grundlegender digitaler Kompetenzen entscheidend ist, um die Bürgerinnen und Bürger angesichts potenzieller Krisen resilienter zu machen. Wie in der Mitteilung der Kommission über

[47] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

die Union der Kompetenzen[48] dargelegt, verfügt knapp die Hälfte der erwachsenen Bevölkerung nicht über grundlegende digitale Kompetenzen, obwohl mehr als 90 % der Arbeitsplätze diese voraussetzen. Um sicherzustellen, dass die derzeitigen und die potenziellen künftigen Arbeitskräfte über die erforderlichen Kompetenzen in einem sich rasch wandelnden digitalen Umfeld verfügen, und um an der Entwicklung der europäischen Talent-Pipeline für den Bereich der Cybersicherheit mitzuwirken, sollte die ENISA Sensibilisierungsmaßnahmen im Bereich der Cybersicherheit unterstützen, die darauf abzielen, Talente anzuwerben und zur Information über die Bildung und die Kompetenzen beizutragen, die im Bereich der Cybersicherheit erforderlich sind, wie z. B. die Europäische Cybersicherheits-Challenge. In diesem Zusammenhang sollte die ENISA Cybersicherheitswettbewerbe, „Capture The Flag"-Bewerbe und ähnliche praktische Übungen koordinieren, um Cybersicherheitskompetenzen und den Kapazitätsaufbau in der gesamten Union zu fördern. Bei der Durchführung von Sensibilisierungsmaßnahmen sollte die ENISA sicherstellen, dass diese den Bedürfnissen nationaler Behörden und von Einrichtungen der Union sowie den Bedürfnissen von Unternehmen, insbesondere von KMU, und von Einrichtungen der allgemeinen und beruflichen Bildung Rechnung tragen, indem sie praktische Rahmen und Schulungen wie „Awareness Raising in a Box" anbietet. Die ENISA sollte zudem praktische und praktisch anwendbare Orientierungshilfen ausarbeiten, um die Umsetzung der Politik und des Rechts der Union im Bereich der Cybersicherheit zu unterstützen. Die ENISA sollte sich außerdem bemühen, relevante Informationen über anwendbare Zertifizierungssysteme verfügbar zu machen, indem sie beispielsweise Leitlinien und Empfehlungen bereitstellt.

(22) Um im Cybersicherheitssektor tätige Unternehmen und Nutzer von Cybersicherheitslösungen zu unterstützen und die wirksame Umsetzung von Titel III dieser Verordnung zu gewährleisten, sollte die ENISA eine „Marktbeobachtungsstelle" aufbauen und pflegen, die die wichtigsten Nachfrage- und Angebotstrends auf dem Cybersicherheitsmarkt regelmäßig analysiert und bekannt macht. Darüber hinaus sollte die ENISA zur Unterstützung der Nutzer der gemäß der Verordnung (EU) 2025/38 eingerichteten EU-Cybersicherheitsreserve im Einklang mit der genannten Verordnung eine Aufstellung der von diesen Nutzern benötigten Dienste und der Verfügbarkeit dieser Dienste ausarbeiten.

(23) Cyberbedrohungen bestehen weltweit. Um die Cybersicherheit zu verbessern, ist eine engere internationale Zusammenarbeit erforderlich, einschließlich der Festlegung gemeinsamer Verhaltensnormen und gemeinsamer Ansätze. Hierzu sollte die ENISA die Zusammenarbeit der Union mit Drittländern – mit Schwerpunkt auf den Ländern, die Kandidaten für den Beitritt zur Union sind – und internationalen Organisationen wie der NATO unterstützen, indem sie der Kommission und den einschlägigen Einrichtungen der Union bei Bedarf die erforderliche Sachkenntnis und die erforderlichen Analysen zur Verfügung stellt. Die internationalen Tätigkeiten der ENISA sollten stets mit den Prioritäten der Union im Einklang stehen.

(24) Um zur Erreichung eines hohen Maßes an Cybersicherheit in der Union beizutragen, sollte die ENISA die operative Zusammenarbeit zwischen den Mitgliedstaaten gemeinsam mit dem CERT-EU sowie die Zusammenarbeit zwischen Einrichtungen der Union und zwischen Interessenträgern unterstützen. Zu diesem Zweck sollte die

[48] Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Die Union der Kompetenzen, COM(2025) 90 final vom 5. März 2025.

Rolle der ENISA gestärkt werden. Die ENISA sollte Mitglied des CSIRTs-Netzwerks werden und zum Austausch und zur Analyse von Informationen im Netzwerk beitragen. Die ENISA sollte zudem die Zusammenarbeit zwischen den jeweiligen CSIRTs bei Vorfällen, Angriffen oder Störungen der von den CSIRTs verwalteten oder geschützten Netze oder Infrastrukturen fördern. Die aktive Unterstützung der Arbeit des CSIRTs-Netzwerks und des Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) durch die ENISA sollte es diesen Netzwerken ermöglichen, ihren Reifegrad weiter zu verbessern. Die Rolle der ENISA bei der Unterstützung einer solchen Zusammenarbeit umfasst die Bekämpfung von Bedrohungen der Sicherheit und Integrität demokratischer Institutionen, Wahlen und anderer Prozesse sowie der kritischen Infrastruktur, auf die sie angewiesen sind, im Einklang mit dem Europäischen Schutzschild für die Demokratie: Förderung starker und widerstandsfähiger Demokratien[49].

(25) Zur Unterstützung des Kapazitätsaufbaus, der operativen Zusammenarbeit und langfristigen strategischen Analysen von Cyberbedrohungen sollte die ENISA die verfügbare technische und operative Sachkenntnis des CERT-EU im Wege einer strukturierten Zusammenarbeit nutzen, z. B. durch spezielle Vereinbarungen.

(26) Um die Cybersicherheit in der gesamten Union zu stärken und eine rasche und wirksame Reaktion auf Cyberbedrohungen zu gewährleisten, sollte die ENISA die Mitgliedstaaten auf deren Ersuchen unterstützen, unter anderem indem sie sie berät, wie sie ihre Fähigkeiten bei der Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen und der Wiederherstellung danach verbessern können, indem sie die technische Bewältigung erheblicher Sicherheitsvorfälle im Sinne der Richtlinie (EU) 2022/2555, insbesondere durch Förderung der freiwilligen Weitergabe technischer Lösungen zwischen den Mitgliedstaaten, erleichtert und indem sie dafür sorgt, dass Cyberbedrohungen und Sicherheitsvorfälle analysiert werden. Die ENISA sollte das EU-CyCLONe auch bei der Erstellung von Berichten für die politische Ebene der Union und der Mitgliedstaaten unterstützen.

(27) Im Hinblick auf eine geringere Exposition gegenüber Einflussnahmen aus dem Ausland, Manipulationen der Lieferketten und Exfiltrationen strategischer Daten sollte die ENISA innerhalb des CSIRTs-Netzwerks und des EU-CyCLONe sichere Kommunikationsinstrumente nutzen. Aufbauend auf der Empfehlung zum Cyberkonzeptentwurf sollten solche Instrumente von Rechtsträgern bereitgestellt werden, die in der Union niedergelassen sind bzw. als in der Union niedergelassen gelten und von Mitgliedstaaten oder von Staatsangehörigen der Mitgliedstaaten kontrolliert werden.

(28) Als Beitrag zur Abwehrbereitschaft und Reaktion auf Unionsebene bei Cybersicherheitsvorfällen und -krisen großen Ausmaßes sollte die ENISA Maßnahmen zur Lageerfassung im Bereich der Cybersicherheit durchführen.

(29) Der Zugang zu verifizierten und zuverlässigen Echtzeit-Erkenntnissen über Cyberbedrohungen ist für eine gemeinsame Lageerfassung in der Union von entscheidender Bedeutung. Die ENISA, die Kommission, der CERT-EU und das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol haben bereits Ablagen mit Erkenntnissen über Cyberbedrohungen erstellt, die auf ihre spezifischen Bedürfnisse zugeschnitten sind. Die ENISA und andere einschlägige Einrichtungen der Union sollten auf freiwilliger Basis zusammenarbeiten, um Ablagen

[49] JOIN(2025) 791 final.

mit verifizierten und zuverlässigen Echtzeit-Erkenntnissen über Cyberbedrohungen zu erstellen, und Synergien ausloten, um Skaleneffekte zu erzielen und die Wirtschaftlichkeit der Haushaltsführung zu verbessern. Diese Arbeit sollte auch sektorale Einrichtungen der Union, wie die EU-Agentur für das Weltraumprogramm, einschließen. Sie sollten nur abgeleitete Analysen, Trends sowie Taktiken, Techniken und Verfahren, aber keine Rohdaten weitergeben und respektieren, dass die Einrichtungen im Einklang mit ihren Mandaten und dem Grundsatz „Kenntnis nur, wenn nötig“ selbst über die Verwaltung des Lebenszyklus ihrer Erkenntnisse über Cyberbedrohungen entscheiden.

(30) Um zu einer zeitnahen und koordinierten Reaktion beizutragen, sollte die ENISA Frühwarnungen an das betreffende CSIRT oder die betreffenden CSIRTs und gegebenenfalls das CSIRTs-Netzwerk und das EU-CyCLONe ausgeben können, wenn Erkenntnisse zu einem erheblichen Sicherheitsvorfall oder einem Sicherheitsvorfall großen Ausmaßes – potenziell oder bereits im Gange – oder einer potenziell grenzübergreifenden Cyberbedrohung vorliegen, insbesondere in Bezug auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Einrichtungen. Informationen im Rahmen solcher Frühwarnungen können öffentlich bekannte Schwachstellen und Angaben darüber enthalten, ob sie Produkte mit digitalen Elementen betreffen, die unter die Verordnung (EU) 2024/2847 fallen, sowie über Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen und Empfehlungen zu Risikominderungsmaßnahmen.

(31) Mit Blick darauf, das Vertrauen zu wahren und die Informationsweitergabe nicht zu gefährden, ist es wichtig, dass die ENISA sichtbare Kennzeichnungen anbringt, aus denen hervorgeht, in welchem Umfang ein von ihr erstelltes oder übermitteltes Dokument oder eine von ihr übermittelte Information weiterverbreitet werden darf. Umgekehrt sollte die ENISA bei der Verwendung von Dokumenten oder Informationen, die sie für die Zwecke der Ausübung ihrer Tätigkeiten erhält, etwaige Einschränkungen durch eine sichtbare Markierung bezüglich der weiteren Verbreitung dieser Informationen beachten.

(32) Um das Bewusstsein für Indikatoren für Cyberbedrohungen und Empfehlungen zu Risikominderungsmaßnahmen zu schärfen, sollte die ENISA Einrichtungen, die in den in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren tätig sind, einen Frühwarndienst bieten. Solche allgemeinen, freiwilligen Frühwarnungen sollten insbesondere KMU zugutekommen und in einem öffentlich zugänglichen maschinenlesbaren Format bereitgestellt werden. In jedem Fall ist ein solcher freiwilliger Dienst unabhängig von jeglicher öffentlich-privater Partnerschaft, die die ENISA möglicherweise einrichtet oder bereits eingerichtet hat, und steht in keinem Zusammenhang mit einer solchen Partnerschaft.

(33) Zur Unterstützung der gemeinsamen Lageerfassung der Union im Bereich der Cybersicherheit sollte die ENISA auf der Grundlage öffentlich verfügbarer Informationen, ihrer eigenen Analysen und anhand von Berichten, die sie von den CSIRTs der Mitgliedstaaten oder den nationalen Anlaufstellen für die Sicherheit von Netz- und Informationssystemen gemäß der Richtlinie (EU) 2022/2555, in beiden Fällen auf freiwilliger Basis, Europol und dem CERT-EU erhalten hat, regelmäßig und in enger Zusammenarbeit mit den Mitgliedstaaten einen eingehenden technischen Lagebericht über die Cybersicherheit in der EU bezüglich Sicherheitsvorfällen und Bedrohungen erstellen. Dieser Bericht sollte dem Rat, dem Europäischen Auswärtigen

Dienst, dem EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission und Europol zur Verfügung gestellt werden.

(34) Um die gemeinsame Lageerfassung der Interessenträger in Bezug auf Cyberbedrohungen und -vorfälle zu verbessern, sollte die ENISA Trends bei Cyberbedrohungen und -vorfällen analysieren. Dies sollte eine regelmäßige Analyse der Sektoren mit hoher Kritikalität und anderer in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführter kritischer Sektoren, einschließlich des Gesundheits-, Energie- und Verkehrssektors, umfassen. Diese Analyse sollte den Reifegrad der Sektoren beinhalten und unter anderem mögliche Herausforderungen ermitteln, die insbesondere in einem bestimmten Sektor auftreten. Um Auswirkungen auf die Lieferkette zu ermitteln, sollten bei der Analyse gegebenenfalls Cyberbedrohungen und -trends im Zusammenhang mit den unter die Verordnung (EU) 2024/2847 fallenden Produktkategorien aufgedeckt werden. Die ENISA sollte Sachkenntnis im Bereich der Cybersicherheit von Infrastrukturen und ihrer kritischen Abhängigkeiten von Lieferketten aufbauen, insbesondere um die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren und die Durchführung der Verordnung (EU) 2024/2847 zu unterstützen. Zu diesem Zweck sollte die ENISA gegebenenfalls auch mit anderen einschlägigen Einrichtungen der Union zusammenarbeiten.

(35) Für ein besseres Verständnis der Herausforderungen im Bereich der Cybersicherheit muss die ENISA zudem aktuelle und neu aufkommende Technologien analysieren und themenspezifische Bewertungen der erwarteten gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Auswirkungen technologischer Innovationen auf die Cybersicherheit vorlegen. Um den Zugang der Öffentlichkeit zu Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen zu erleichtern, kann die ENISA relevante Informationen auf ihrer Website benutzerfreundlich und gut strukturiert bereitstellen.

(36) Die gestärkte Rolle der ENISA bei der Förderung der Lageerfassung, der Bedrohungsanalyse und der Bereitstellung technischer Beratung wird helfen, die kollektiven Cybersicherheitsbemühungen in Bezug auf Produkte mit digitalen Elementen auszuweiten und die Durchführung der Verordnung (EU) 2024/2847 zu unterstützen. Gemäß der Verordnung (EU) 2024/2847 kann die ENISA den Marktüberwachungsbehörden gemeinsame Tätigkeiten zur Überprüfung der Konformität von Produkten mit digitalen Elementen vorschlagen und Kategorien von Produkten mit digitalen Elementen ermitteln, für die koordinierte Kontrollen (Sweeps) durchgeführt werden können. Informationen aus der Analyse von Cyberbedrohungen und aus Frühwarnungen sollten zu einer verstärkten Unterstützung dieser Behörden durch die ENISA führen und zu einer wirksamen Durchsetzung der Verordnung (EU) 2024/2847 beitragen, um Auswirkungen von Cyberangriffen auf die Lieferketten im gesamten Binnenmarkt zu verhindern und die Abwehrbereitschaft der Union insgesamt zu verbessern.

(37) Ransomware-Angriffe stellen eine große Bedrohung der Cybersicherheit für die Union dar. Um die Cybersicherheit der Union zu erhöhen und Ransomware zu bekämpfen, sollte die ENISA Fähigkeiten zur Lageerfassung und zur Unterstützung der Reaktion auf Sicherheitsvorfälle und die Wiederherstellung danach entwickeln. Bei der Unterstützung einzelner wesentlicher und wichtiger Einrichtungen bei der Reaktion auf einen Ransomware-Angriff und der Wiederherstellung danach sollte die ENISA eng mit Europol und gegebenenfalls mit den CSIRTs oder den zuständigen Behörden zusammenarbeiten und sich dabei auf die langjährige Erfahrung von Europol bei der

Bekämpfung von Ransomware-Angriffen stützen. Dies sollte die Arbeit der CSIRTs zur Unterstützung der Reaktion auf Sicherheitsvorfälle ergänzen. Um bei ihrem Kampf gegen Ransomware Synergien zu erzielen, sollte die ENISA einen Helpdesk einrichten und zu diesem Zweck einschlägige Fähigkeiten und Dienste zur Bekämpfung von Ransomware bündeln und Informationen, Leitlinien und Instrumente leicht zugänglich machen, die wesentlichen und wichtigen Einrichtungen bei der Reaktion auf einen Ransomware-Vorfall und der Wiederherstellung danach helfen können.

(38) Die ENISA sollte der Kommission technische Sachkenntnis und Unterstützung bereitstellen, indem sie ein jährliches fortlaufendes Programm von Cybersicherheitsübungen auf Unionsebene im Einklang mit der Empfehlung zum Cyberkonzeptentwurf ausarbeitet, um auf Cyberkrisen vorbereitet zu sein, das Cybersicherheitsniveau von Einrichtungen, die an solchen Übungen teilnehmen, zu testen und Doppelarbeit zu verringern. So sollte die ENISA beispielsweise beraten, welche Arten von Übungen – Planübungen, hybride Übungen oder Übungen unter Realbedingungen – mit welchen Zielen, Szenarien und Teilnehmern geeignet wären.

(39) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen und ein robustes Schwachstellenmanagement sind unerlässlich, um ein hohes Maß an Cybersicherheit im Binnenmarkt zu gewährleisten. Aus diesem Grund sollte die ENISA eine europäische Schwachstellendatenbank gemäß der Richtlinie (EU) 2022/2555 pflegen und einen gemeinsamen Schwachstellenmanagementdienst der Union einrichten, um ein robustes und nachhaltiges Diensteniveau zu gewährleisten und das Risiko von Störungen zu verringern. Hierzu sollte die ENISA Möglichkeiten prüfen, die strukturierte Zusammenarbeit mit Programmen, Registern oder Datenbanken, die der europäischen Schwachstellendatenbank ähneln, zu vertiefen, um Doppelarbeit zu vermeiden und gegebenenfalls Komplementarität auf internationaler Ebene anzustreben. Darüber hinaus sollte die ENISA die von mehreren Parteien koordinierte Offenlegung von Schwachstellen auf Unionsebene unterstützen und Mehrwertdienste wie Beratung zu Schwachstellen, Bewertung des Schweregrads und Produktlisten sowie einen verbesserten europäischen Katalog bekannter ausgenutzter Schwachstellen bereitstellen, um die Einrichtungen in ihrem Schwachstellenmanagement zu unterstützen.

(40) Die Rolle der ENISA bei der Weiterentwicklung des ECCF sollte ein zentrales Element ihres Mandats sein. Die ENISA sollte während des gesamten Lebenszyklus der europäischen Systeme für die Cybersicherheitszertifizierung ihre technische Sachkenntnis zur Verfügung stellen. Im Hinblick auf ein künftiges System sollte die ENISA bestehende Normen oder technische Spezifikationen ermitteln, auf denen ein System aufbauen kann, und gegebenenfalls selbst Entwürfe technischer Spezifikationen erstellen, auf die in einem System Bezug genommen werden kann. Die ENISA sollte damit beauftragt werden, auf Ersuchen der Kommission mögliche Systeme auszuarbeiten. Zudem sollte die ENISA für die Pflege bereits bestehender Systeme zuständig sein. Dabei sollte die ENISA zum Aufbau und zur Entwicklung eines Zertifizierungsökosystems beitragen, über das Mitgliedstaaten und private Interessenträger Rückmeldungen geben können und deren Zertifizierungskapazitäten gestärkt werden. Dies sollte auch den Betrieb einer eigenen Zertifizierungswebsite umfassen, auf der einschlägige Informationen im Zusammenhang mit angenommenen Systemen, einschließlich Zertifikaten und Konformitätserklärungen, frei und öffentlich zugänglich sind.

(41) Um die Umsetzung der einschlägigen Rechtsvorschriften der Union zu unterstützen, sollte die ENISA die aktuelle Technik im Bereich der Cybersicherheit gestalten, indem sie technische Spezifikationen zur Unterstützung der Umsetzung der einschlägigen Rechtsvorschriften der Union bereitstellt, auch im Hinblick darauf, dass in europäischen Systemen für die Cybersicherheitszertifizierung auf sie Bezug genommen werden kann. Die ENISA sollte außerdem die Ausarbeitung und Weiterentwicklung von Normen durch die einschlägigen Normungsgremien überwachen, um die Normungstrends auf europäischer und globaler Ebene zu verfolgen und diese Normen bei Bedarf mitzugestalten, indem sie sich – auch durch die Ausarbeitung von Beiträgen – an den Tätigkeiten der Normungsorganisationen beteiligt und eine führende Rolle übernimmt. Dabei sollte die ENISA unparteiisch bleiben. So könnte es beispielsweise Situationen geben, in denen sich die ENISA von bestimmten Tätigkeiten in Normungsgremien zurückziehen sollte, wenn die ENISA beauftragt wird, europäische Normen zu bewerten, die die Kommission zur Unterstützung der Rechtsvorschriften der Union in Auftrag gegeben hat. Die ENISA sollte nicht zur Ausarbeitung von Normen beitragen, für deren Bewertung sie zuständig ist.

(42) Um die Umsetzung der Unionspolitik und die Vorbereitung potenzieller Normungstätigkeiten zu unterstützen, sollte die ENISA zur Entwicklung und Bewertung kryptografischer Algorithmen beitragen, insbesondere im Bereich der Post-Quanten-Kryptografie. In diesem Zusammenhang kann die ENISA auf Ersuchen der Kommission und vorbehaltlich einer Beitragsvereinbarung im Sinne der Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates[50] ein Verfahren zur Anforderung und Bewertung von Algorithmen für kryptografische Algorithmen durch einschlägige Interessenträger, insbesondere aus der Welt der Kryptografie, aus Wissenschaft und Forschung sowie Hersteller, CSIRTs, nationale Behörden für die Cybersicherheitszertifizierung und zuständige Behörden gemäß der Richtlinie (EU) 2022/2555, einrichten. Trägt die ENISA zur Einrichtung solcher Verfahren bei, sollte sie die Zusammenarbeit zwischen den betreffenden Interessenträgern fördern und sich um die organisatorischen Aspekte kümmern. Das Verfahren sollte förmlich, offen, transparent und inklusiv sein und auch die Konsultation der betreffenden Interessenträger zu Entwürfen von Mindestanforderungen sowie zum Bewertungsverfahren und den Bewertungskriterien, insbesondere was die Sicherheit und die Durchführung von Bewertungen betrifft, umfassen.

(43) Um die Durchführung von Konformitätsbewertungstätigkeiten im Rahmen der europäischen Systeme für die Cybersicherheitszertifizierung und anderer einschlägiger Rechtsvorschriften der Union zu unterstützen, kann die ENISA relevante technische Testinstrumente bereitstellen, um die Mitgliedstaaten, Unternehmen und Konformitätsbewertungsstellen bei Bewertungstätigkeiten zu unterstützen. Diese Instrumente sollten auf Synergien auf Unionsebene und auf eine effiziente Durchführung von Konformitätsbewertungsverfahren abzielen, um dem Bedarf der Mitgliedstaaten und des Marktes gerecht zu werden. Ein solcher Bedarf kann sich beispielsweise im Bereich der konzeptionsintegrierten Sicherheit ergeben, um Unternehmen, einschließlich kleiner und mittlerer Unternehmen, in ihren Bemühungen zur Umsetzung der Verordnung (EU) 2024/2847 zu unterstützen. In diesem

[50] Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates vom 23. September 2024 über die Haushaltsordnung für den Gesamthaushaltsplan der Union (ABl. L, 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

Zusammenhang sollte die ENISA Gebühren erheben, um die einschlägigen Kosten im Zusammenhang mit der Einrichtung, Konzeption, Entwicklung, Pflege und Aktualisierung der erforderlichen Software- und Hardwarekapazitäten für solche Testinstrumente zu decken.

(44) Um die Mitgliedstaaten in ihren Bemühungen zu unterstützen, dem Mangel an Cybersicherheitsfachkräften und dem wachsenden Bedarf an qualifizierten, flexiblen und – auch hinsichtlich eines ausgewogenen Geschlechterverhältnisses – vielfältigen Arbeitskräften zu begegnen, und um die Mobilität der Arbeitskräfte und die Abwehrbereitschaft in allen Mitgliedstaaten zu verbessern, sollte die ENISA auf den Grundsätzen und Arbeiten aufbauen, die im Rahmen der Akademie für Cybersicherheitskompetenzen bereits initiiert wurden. Insbesondere sollte die ENISA den europäischen Rahmen für Cybersicherheitskompetenzen (ECSF) als gemeinsamen Rahmen für Rollenprofile von Cybersicherheitsfachkräften etablieren. Darüber hinaus sollte die ENISA die Mitgliedstaaten dabei unterstützen, geschlechtsspezifische Unterschiede bei den Aufgaben im Bereich der Cybersicherheit zu überwinden. Dieser Ansatz steht im Einklang mit der in der Mitteilung der Kommission über die Union der Kompetenzen dargelegten Vision und würde zu deren Zielen beitragen. Zudem sollte ein Qualitätssiegel für europäische Einzelbescheinigungen von Cybersicherheitskompetenzen geprüft werden.

(45) Der ECSF sollte ein praktisches und flexibles Instrument sein, das auf freiwilliger Basis eingesetzt werden kann und ein gemeinsames Verständnis und eine gemeinsame Terminologie der einschlägigen Rollen und der damit verbundenen Aufgaben, Fähigkeiten und Kenntnisse bietet, die für Cybersicherheitsfunktionen hauptsächlich erforderlich sind, um bei der Ermittlung kritischer Kompetenzen, einschließlich Querschnittskompetenzen, die die Arbeitskräfte mitbringen müssen, zu helfen, Bildungsanbietern, einschließlich Unternehmen, Hochschuleinrichtungen oder Anbietern beruflicher Aus- und Weiterbildung, die Erstellung von Programmen zu ermöglichen und politische Entscheidungsträger bei der Entwicklung von Initiativen zur Schließung von Kompetenzlücken zu unterstützen. Da der ECSF auch als Referenzrahmen für die Anerkennung von Kompetenzen genutzt werden könnte, sollte er auch mit der europäischen Klassifizierung für Fähigkeiten/Kompetenzen, Qualifikationen und Berufe (ESCO) interoperabel sein, damit Personalabteilungen die Anforderungen an die Ressourcenplanung, Einstellung und Laufbahnentwicklung im Bereich der Cybersicherheit verstehen können. Während DigComp 3.0 die Kenntnisse, Fähigkeiten und Einstellungen beschreibt, die als digitale Kompetenzen für das tägliche Leben, die Teilhabe an der Gesellschaft, die Arbeit und das Lernen benötigt werden, und sowohl von Erwachsenen als auch von Kindern genutzt werden kann, bietet der ECSF einen einfachen Rahmen für die Ermittlung von Cybersicherheitsfunktionen und damit verbundenen Aufgaben, Kenntnissen und Fähigkeiten, die für die Erfüllung dieser Funktionen erforderlich sind. Dabei richtet er sich an Cybersicherheitsfachkreise von tatsächlichen oder potenziellen Cybersicherheitsfachkräften über Bildungseinrichtungen bis hin zu Arbeitgebern. Darüber hinaus sollte der ECSF auch zur Entwicklung europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen beitragen, indem er als wichtigstes Instrument für die Entwicklung der Systeme dient, durch die neue Marktteilnehmer auftreten können und der Wettbewerb auf dem Markt innerhalb eines gemeinsamen Rahmens unterstützt wird. Der ECSF sollte regelmäßig bewertet und aktualisiert werden, um sicherzustellen, dass er dem Arbeitsmarktbedarf im Bereich der Cybersicherheit sowie den technologischen und politischen Entwicklungen angemessen Rechnung trägt. Die ENISA sollte die Inanspruchnahme des ECSF durch

die und in den Mitgliedstaaten und Einrichtungen der Union fördern und bei Bedarf angemessene Unterstützung leisten.

(46) Kompetenzen und Qualifikationen im Bereich der Cybersicherheit sollten im gesamten Binnenmarkt vergleichbar, transparent und vertrauenswürdig sein. Zu diesem Zweck sollten europäische Einzelbescheinigungen von Cybersicherheitskompetenzen[51] Arbeitgebern, einschließlich KMU und Start-up-Unternehmen, dabei helfen, im Einklang mit den Zielen gemäß der Mitteilung über die Union der Kompetenzen tatsächliche oder potenzielle Cybersicherheitsfachkräfte innerhalb eines Mitgliedstaats oder aus anderen Mitgliedstaaten wirksam einzustellen. Um eine einheitliche Umsetzung in allen Mitgliedstaaten zu gewährleisten, sollten europäische Einzelbescheinigungen von Cybersicherheitskompetenzen auf einem unionsweit gemeinsamen Verständnis der zur Erreichung dieser Ziele erforderlichen Kompetenzen beruhen und von Anbietern, die von der ENISA zugelassen wurden, auf der Grundlage gemeinsamer Kriterien ausgestellt werden. Dieser Ansatz sollte mit den Zielen der künftigen Initiative für die Portabilität von Kompetenzen im Einklang stehen und zu ihnen beitragen.

(47) Die Entwicklung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen sollte darauf abzielen, die Maßnahmen der Mitgliedstaaten dadurch zu ergänzen, dass Behörden und Wirtschaftsteilnehmer die Möglichkeit erhalten, im Einklang mit der unterstützenden Zuständigkeit der Union im Bereich der allgemeinen und beruflichen Bildung gemäß Artikel 6 Buchstabe e, Artikel 165 Absatz 1 und Artikel 166 Absatz 1 AEUV einen europäischen Bescheinigungsmechanismus zu nutzen. Die Systeme können zusammen mit der Arbeit der Akademie für Cybersicherheitskompetenzen auch die Grundlage für Hochschulprogramme, wie europäische Studiengänge in diesem Bereich, und für die Entwicklung von Microcredentials bilden. Daher sollten die Systeme europäischer Bescheinigungen individueller Cybersicherheitskompetenzen nicht darauf abzielen, die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zu harmonisieren, sondern vielmehr als Wegbereiter und Chance betrachtet werden, die die Mitgliedstaaten und Wirtschaftsteilnehmer möglicherweise nutzen und voranbringen wollen.

(48) Die ENISA sollte sicherstellen, dass die Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen weiterhin dem Marktbedarf entsprechen und auf den Erfahrungen sowohl öffentlicher als auch privater Anbieter individueller Zertifizierungen, einschließlich Mitgliedstaaten, Hochschuleinrichtungen, Einrichtungen der beruflichen Aus- und Weiterbildung und Unternehmen, aufbauen. Die ENISA sollte die Kommission zur Priorisierung der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen konsultieren und dabei die Erfordernisse der politischen Umsetzung und des Marktes gebührend berücksichtigen.

(49) Um für Kohärenz zwischen dem ECSF und den Systemen zu sorgen, sollte die Überarbeitung eines ECSF-Rollenprofils automatisch eine Bewertung der Zweckmäßigkeit des damit verbundenen Systems oder der damit verbundenen

---

[51] Die europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen sind so zu verstehen, dass sie einem ähnlichen Ansatz folgen wie die auf dem Markt anerkannten „Cybersicherheitszertifizierungen“. Um jedoch Verwirrung in Bezug auf den europäischen Rahmen für die Cybersicherheitszertifizierung zu vermeiden, wird der bereits in der Mitteilung über die Akademie für Cybersicherheitskompetenzen verwendete Begriff „Bescheinigung“ bevorzugt.

Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen nach sich ziehen, was zu einer Überprüfung des Systems bzw. der Systeme führen kann.

(50) Angesichts der Vielfalt der Rollenprofile im Bereich der Cybersicherheit und der damit verbundenen Aufgaben, Fähigkeiten und Kenntnisse müssen die Bewertung von Einzelpersonen und die Bewertungsmethoden möglicherweise in jedem einzelnen System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen angepasst werden. In jedem System sollte sichergestellt sein, dass die Bewertung der erforderlichen Kompetenzen einer Person in Bezug auf die Lernergebnisse, gegebenenfalls einschließlich der Bewertung des Kompetenzniveaus, systematisch anhand eines ECSF-Rollenprofils oder einer Teilmenge davon erfolgt. Bewertungsmethoden können Elemente wie die Prüfung theoretischer Kenntnisse, praktische Prüfungen, die Bewertung von Voraussetzungen und gegenseitige Bewertung umfassen. Die Erfahrung der jeweiligen Person sollte gebührend berücksichtigt werden.

(51) Um eine einheitliche Umsetzung der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, insbesondere im Hinblick auf die Bewertung von Einzelpersonen, zu gewährleisten, sollte die ENISA obligatorische Schulungen für das Personal anbieten, das für die Durchführung der Bewertung von Einzelpersonen zuständig ist. Dieses Personal sollte über Erfahrung im Bereich der Cybersicherheit, nachgewiesen durch eine europäische Einzelbescheinigung von Cybersicherheitskompetenzen für das Rollenprofil, für das es die Bewertung durchführt, und über ein Kompetenzniveau verfügen, das mindestens dem der von ihm zu bewertenden Einzelpersonen entspricht.

(52) Die Aufgabe der befugten Bescheinigungsanbieter besteht darin, zu bescheinigen, dass eine Einzelperson über die Kenntnisse und Kompetenzen verfügt, eine der ECSF-Rollen wahrzunehmen, und Arbeitgebern in der gesamten Union Gewissheit zu geben. Da auch Arbeitgeber, die kritische Infrastrukturen in der Union betreiben, Gewissheit bezüglich des Fähigkeits- und Kompetenzniveaus von Einzelpersonen im Besitz einer europäischen Einzelbescheinigung von Cybersicherheitskompetenzen anstreben werden, sollten die befugten Anbieter, die das Fähigkeits- und Kompetenzniveau bescheinigen, unter dem Gesichtspunkt der Cybersicherheit vertrauenswürdig sein und nicht der unzulässigen Einflussnahme durch ein Drittland unterliegen, für das Cybersicherheitsbedenken bestehen könnten. Daher sollten Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen und das gemäß dieser Verordnung benannt wurde, niedergelassen sind oder die von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands (Hochrisikoanbieter) entsprechend dieser Verordnung kontrolliert werden, keine befugten Bescheinigungsanbieter von europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Titel II Abschnitt 4 werden können.

(53) Damit Einzelpersonen, die über eine europäische Bescheinigung von Cybersicherheitskompetenzen verfügen, diese leicht verwenden und vorlegen können und damit eine solche Bescheinigung in allen Mitgliedstaaten verwendet werden kann, sollten befugte Bescheinigungsanbieter sicherstellen, dass auf Ersuchen der betreffenden Einzelperson elektronische Ausfertigungen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen an die mit der Verordnung (EU) Nr. 910/2014 eingeführte europäische Brieftasche für die digitale Identität (EUid-Brieftasche) ausgestellt werden. Befugte Bescheinigungsanbieter sollten als Vertrauensdiensteanbieter gelten und der Aufsichts- und Haftungsregelung gemäß der

Verordnung (EU) Nr. 910/2014 unterliegen. Die gemäß der Durchführungsverordnung (EU) 2025/1569 der Kommission[52] genutzte Attributsbescheinigungsregelung sollte im Katalog der Attributsbescheinigungsregelungen gemäß der genannten Durchführungsverordnung registriert sein.

(54) Um zur Entwicklung der Fachkräftebasis im Bereich der Cybersicherheit und zur Portabilität von Kompetenzen in der gesamten Union beizutragen, sollte die ENISA die Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen und die Liste der befugten Bescheinigungsanbieter über eine eigene Website öffentlich zugänglich machen.

(55) Bei der Leitung und beim Betrieb der ENISA sollten die Grundsätze des am 19. Juli 2012 vom Europäischen Parlament, vom Rat und von der Kommission angenommenen gemeinsamen Konzepts für die dezentralen Agenturen der Union[53] berücksichtigt werden. Die im Gemeinsamen Konzept enthaltenen Empfehlungen sollten gegebenenfalls auch in den Arbeitsprogrammen, den Bewertungen und den Berichterstattungs- und Verwaltungsverfahren der ENISA zur Geltung kommen.

(56) Damit der Verwaltungsrat seine Aufgaben, insbesondere die allgemeine Ausrichtung der Tätigkeiten der ENISA und die Festlegung ihrer strategischen Prioritäten, wirksam erfüllen kann, ist es von wesentlicher Bedeutung, dass sich der Verwaltungsrat aus hochrangigen Vertretern der Mitgliedstaaten und der Kommission zusammensetzt. Hierzu sollte jeder Mitgliedstaat den Leiter einer gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten für die Cybersicherheit zuständigen nationalen Behörde des Mitgliedstaats als Mitglied des Verwaltungsrats ernennen.

(57) Um sicherzustellen, dass die stellvertretenden Mitglieder des Verwaltungsrats ihre Aufgaben angemessen erfüllen können, sollten die Mitgliedstaaten stellvertretende Mitglieder benennen, die über angemessene Sachkenntnis und Erfahrung verfügen. Die Kommission und die Mitgliedstaaten sollten sich in Bezug auf Stellvertreter um eine ausgewogene Vertretung von Männern und Frauen im Verwaltungsrat bemühen und sollten die Fluktuation gering halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen.

(58) Damit die ENISA ihrem Auftrag wirksam nachkommen kann, sollte der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, die allgemeine Ausrichtung der Tätigkeit der ENISA, einschließlich ihrer strategischen Prioritäten, festlegen und dafür sorgen, dass sie ihre Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte über die erforderlichen Befugnisse verfügen, um den Haushaltsplan aufzustellen und die Ausführung des Haushaltsplans zu überprüfen, angemessene Finanzvorschriften und transparente Verfahren für die Entscheidungsfindung der ENISA festzulegen, das einheitliche Programmplanungsdokument der ENISA anzunehmen, sich eine Geschäftsordnung zu geben, den Exekutivdirektor zu ernennen, über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen und zu entscheiden, ob der Posten eines stellvertretenden Exekutivdirektors geschaffen wird,

---

52 Durchführungsverordnung (EU) 2025/1569.

53 Gemeinsames Konzept im Anhang der Gemeinsamen Erklärung des Europäischen Parlaments, des Rates der EU und der Europäischen Kommission zu den dezentralen Agenturen, angenommen am 19. Juli 2012, abrufbar unter: https://european-union.europa.eu/document/download/d4199ff4-1e3d-45e6-af7e-90cf1a7b10bc_en?filename=joint_statement_on_decentralised_agencies_en.pdf.

und, wenn dieser Posten geschaffen wird, über die Ernennung sowie die Verlängerung und die Beendigung der Amtszeit zu entscheiden. Jede Person, die innerhalb der ENISA eine Führungsaufgabe wahrnimmt, sollte daher vom Verwaltungsrat ernannt werden. Der Verwaltungsrat sollte auch für die Ernennung oder Abberufung von Mitgliedern der Beschwerdekammer sowie für die Festlegung von Vorschriften zur Vermeidung oder Bewältigung diesbezüglicher Interessenkonflikte zuständig sein.

(59) Um sicherzustellen, dass die ENISA ihre strategischen Prioritäten festlegt und auf dem neuesten Stand hält, sollte der Verwaltungsrat mindestens eine Sitzung pro Jahr zum Thema der strategischen Prioritäten der ENISA abhalten. Damit die Sitzungen des Verwaltungsrats wirkungsvoll sind und die Teilnehmer über fundierte Informationen verfügen, kann der Verwaltungsrat zu seinen Sitzungen jede Person einladen, deren Stellungnahme für die erörterten Themen relevant und von Interesse sein könnte, um Einblicke, Sachkenntnis oder Beratung zu erhalten. Eine solche Person wäre ein Ad-hoc-Beobachter ohne Stimmrecht.

(60) Sofern in dieser Verordnung nichts anderes bestimmt ist, sollte der Verwaltungsrat Beschlüsse mit absoluter Mehrheit seiner stimmberechtigten Mitglieder fassen. Aufgrund der Bedeutung von Haushalts- und Personalangelegenheiten, insbesondere Angelegenheiten im Zusammenhang mit dem jährlichen Haushaltsplan, dem jährlichen Tätigkeitsbericht, der Betrugsbekämpfungsstrategie, den Durchführungsbestimmungen zum Statut, der Ernennung des Exekutivdirektors, des stellvertretenden Exekutivdirektors und des Rechnungsführers, der Weiterverfolgung der Feststellungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und der Europäischen Staatsanwaltschaft (EUStA) sowie der Annahme der Finanzregelung der ENISA, sollte der Verwaltungsrat solche Beschlüsse nur fassen, wenn der Vertreter der Kommission zustimmt. Ein Beschluss über die Annahme eines endgültigen einheitlichen Programmplanungsdokuments nach Berücksichtigung der Stellungnahme der Kommission bedarf nur für die Elemente des Beschlusses eines zustimmenden Votums des Vertreters der Kommission, die nicht mit dem jährlichen und mehrjährigen Arbeitsprogramm der ENISA in Zusammenhang stehen.

(61) Der Exekutivrat sollte dazu beitragen, dass der Verwaltungsrat effektiv arbeiten kann. Im Rahmen seiner vorbereitenden Arbeiten für die Beschlüsse des Verwaltungsrats sollte der Exekutivrat die einschlägigen Informationen im Detail prüfen und die sich bietenden Optionen sondieren; zudem sollte er die einschlägigen Beschlüsse des Verwaltungsrats vorbereiten, indem er Beratung und Lösungen anbietet. Er sollte außerdem den Exekutivdirektor bei der Umsetzung der Beschlüsse des Verwaltungsrats unterstützen und beraten.

(62) Damit die ENISA reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird und über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt. Die Aufgaben des Exekutivdirektors sollten in völliger Unabhängigkeit wahrgenommen werden. Der Verwaltungsrat sollte den Exekutivdirektor aus der von der Kommission erstellten Kandidatenliste in einem offenen und transparenten Verfahren ernennen, das dem Grundsatz der ausgewogenen Vertretung von Frauen und Männern Rechnung trägt.

(63) Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das einheitliche Programmplanungsdokument der ENISA ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Er sollte einen dem Verwaltungsrat vorzulegenden Jahresbericht, in dem auch die

Umsetzung des jährlichen Arbeitsprogramms der ENISA behandelt wird, ausarbeiten, einen Entwurf eines Voranschlags für die Einnahmen und Ausgaben der ENISA erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder sozioökonomischen Einzelfragen befassen. Insbesondere im Zusammenhang mit der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung (im Folgenden „mögliches System“) wird die Einrichtung einer Ad-hoc-Arbeitsgruppe für notwendig erachtet. Die Einsetzung einer Ad-hoc-Arbeitsgruppe könnte auch für Tätigkeiten zur Pflege bestimmter angenommener europäischer Systeme für die Cybersicherheitszertifizierung erforderlich sein. Außerdem sollten Ad-hoc-Arbeitsgruppen eingesetzt werden, um Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen zu entwickeln und zu pflegen und die Agentur bei der Governance, Umsetzung und Weiterentwicklung des ECSF zu unterstützen. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen, dass ein ausgewogenes Verhältnis von Frauen und Männern besteht und dass je nach behandelter Einzelfrage gegebenenfalls ein angemessenes Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Einrichtungen der Union, dem Privatsektor, einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit, sowie wissenschaftlichen Sachverständigen für Produkte mit digitalen Elementen gewahrt wird.

(64) Der Verwaltungsrat kann beschließen, einen stellvertretenden Exekutivdirektor einzusetzen, der den Exekutivdirektor unterstützt, wenn der Verwaltungsrat der Auffassung ist, dass ein solcher Posten erforderlich ist, um das reibungslose Funktionieren der ENISA sicherzustellen oder aufrechtzuerhalten. Bei der Entscheidung darüber, ob dieser Posten geschaffen werden soll, kann der Verwaltungsrat die Stellungnahme des Exekutivdirektors berücksichtigen.

(65) Die ENISA sollte über eine Beratungsgruppe verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, den Verbraucherorganisationen und sonstigen relevanten Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte ENISA-Beratungsgruppe sollte hauptsächlich Fragen behandeln, die die Interessenträger betreffen, und diese der ENISA zur Kenntnis bringen. Die ENISA-Beratungsgruppe sollte vor allem im Hinblick auf den Entwurf des jährlichen Arbeitsprogramms der ENISA hinzugezogen werden. Die Zusammensetzung der ENISA-Beratungsgruppe und die dieser Gruppe übertragenen Aufgaben, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der ENISA ausreichend vertreten sind. Vertreter der Strafverfolgungs-, Datenschutz- und Marktüberwachungsbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der ENISA-Beratungsgruppe infrage kommen.

(66) Antragsteller, die befugte Bescheinigungsanbieter werden oder ihre Befugnis verlängern lassen möchten, sollten Zugang zu den erforderlichen Rechtsbehelfen haben, wenn sie von Entscheidungen der ENISA betroffen sind. Deshalb sollte ein geeignetes Beschwerdeverfahren eingerichtet werden, damit die betreffenden Entscheidungen der ENISA vor einer Beschwerdekammer angefochten werden können, deren Entscheidungen gemäß den Verträgen einer gerichtlichen Überprüfung durch den Gerichtshof der Europäischen Union unterzogen werden können. Das Erfordernis, das Beschwerdeverfahren innerhalb der ENISA auszuschöpfen, bevor der

Gerichtshof der Europäischen Union mit der Klage befasst wird, gilt nur für Personen, die bei der Beschwerdekammer klagebefugt sind.

(67) Um die vollständige Selbstständigkeit und Unabhängigkeit der ENISA sicherzustellen und sie in die Lage zu versetzen, ihre Aufgaben zu erfüllen, sollte die ENISA mit einem ausreichenden und eigenständigen Haushalt ausgestattet werden, der in erster Linie aus einem Beitrag der Union, aber auch aus Beiträgen von Drittländern, die sich an der Arbeit der ENISA beteiligen, und aus Gebühren finanziert wird, die von befugten Bescheinigungsanbietern und von Konformitätsbewertungsstellen entrichtet werden, die an Systemen teilnehmen und europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen ausstellen. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zum Haushaltsplan der ENISA zu leisten. Bei der ENISA eingehende Beiträge – ob finanzieller Natur oder als Sachleistungen – von Mitgliedstaaten, Drittländern oder anderen Einrichtungen oder Personen sollten die Unabhängigkeit und Unparteilichkeit der Agentur nicht beeinträchtigen. Das Haushaltsverfahren der Union sollte Anwendung finden, soweit der Beitrag der Union und etwaige andere Zuschüsse aus dem Gesamthaushaltsplan der Union betroffen sind. Die Rechnungsführung der ENISA sollte durch den Rechnungshof geprüft werden, um Transparenz und Rechenschaftspflicht sicherzustellen. Damit sich die Agentur in Zukunft an allen relevanten Projekten beteiligen kann, sollte sie die Möglichkeit haben, Finanzhilfen zu erhalten.

(68) Damit die ENISA die Nachfrage nach den von ihr durchgeführten Tätigkeiten erfüllen kann, insbesondere in Bezug auf Entscheidungen, mit denen Anbietern die Befugnis erteilt wird, europäische Einzelbescheinigungen von Cybersicherheitskompetenzen auszustellen, und in Bezug auf die Pflege der europäischen Systeme für die Cybersicherheitszertifizierung und der Testinstrumente, sollte die ENISA die Befugnis erhalten, Gebühren zu erheben. Die Gebühren im Zusammenhang mit der Bearbeitung von Anträgen auf Zulassung als befugter Bescheinigungsanbieter sollten angemessen festgesetzt werden, um einen ausreichenden Beitrag zur Deckung der geschätzten Kosten für die Entwicklung und Pflege der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen zu leisten und zu bewerten, ob den Anforderungen und Verpflichtungen für befugte Bescheinigungsanbieter (weiterhin) nachgekommen wird. Die Gebühren im Zusammenhang mit den Kosten für die Erteilung und Verlängerung von Befugnissen für befugte Bescheinigungsanbieter sollten auch Kosten im Zusammenhang mit Bewertungen einschließen, die von der ENISA oder unter ihrer Aufsicht durchgeführt werden. Die Gebühren im Zusammenhang mit der Teilnahme an europäischen Systemen für die Cybersicherheitszertifizierung und für die Ausstellung von Zertifikaten im Rahmen dieser Systeme sollten angemessen festgesetzt werden, um einen ausreichenden Beitrag zur Deckung der geschätzten Kosten für die Aufrechterhaltung solcher Systeme zu leisten. Die Zahlung dieser Gebühren sollte es notifizierten Konformitätsbewertungsstellen und gegebenenfalls Inhabern von im Rahmen eines Systems ausgestellten Zertifikaten ermöglichen, sich an solchen Tätigkeiten sowie an relevanten Kapazitätsaufbau- und Werbemaßnahmen zu beteiligen, um den Austausch bewährter Verfahren und die Einführung von Systemen und zertifizierten Lösungen zu fördern.

(69) Um Verhältnismäßigkeit, Transparenz und Rechtssicherheit zu gewährleisten, sollten die Gebühren transparent und fair festgesetzt werden. Alle Ausgaben der ENISA für Personal, das an gebührenpflichtigen Tätigkeiten beteiligt ist, insbesondere die anteiligen Beiträge des Arbeitgebers zur Altersvorsorge, sowie die Kosten im

Zusammenhang mit der Beschwerdekammer werden bei diesen Kosten berücksichtigt. Die Gebühren dürfen nicht dazu führen, dass den Antragstellern unnötige finanzielle Belastungen oder unnötiger Verwaltungsaufwand auferlegt werden. Für die Gebühren sollten angemessene Zahlungsfristen festgelegt werden.

(70) Es ist erforderlich, eine Reihe von Indikatoren einzuführen, um die Arbeitsbelastung, Wirksamkeit und Effizienz der Agentur in Bezug auf die durch Gebühren finanzierten Tätigkeiten zu messen. Mit Blick auf diese Indikatoren passt die Agentur ihre Personalplanung und die Verwaltung der Ressourcen aus Gebühren an, um auf eine solche Nachfrage und etwaige Schwankungen bei den Einnahmen aus Gebühren angemessen reagieren zu können.

(71) Damit mutmaßliche oder tatsächliche Interessenkonflikte festgestellt und ordnungsgemäß behoben werden können, sollten bei der ENISA Vorschriften zur Vermeidung von und zum Umgang mit Interessenkonflikten gelten. Die ENISA sollte auch die Vorschriften für den Zugang zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates[54] anwenden. Die Verarbeitung personenbezogener Daten durch die ENISA sollte nach der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[55] erfolgen. Die ENISA sollte die für die Einrichtungen der Union geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der Europäischen Union (EUCI), sowie die entsprechenden nationalen Rechtsvorschriften befolgen.

(72) Bei der Wahrnehmung ihrer Aufgaben kann die ENISA Zugang zu sensiblen Informationen haben, z. B. zu Informationen über Cyberbedrohungen und Sicherheitsvorfälle. Daher ist es entscheidend, dass die ENISA die Vertraulichkeit der von ihr verarbeiteten Informationen wahrt. Insbesondere sollten die Beamten und sonstigen Bediensteten der ENISA gemäß Artikel 339 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) auch nach Beendigung ihrer Amtstätigkeit keine Auskünfte, die ihrem Wesen nach unter das Berufsgeheimnis fallen, preisgeben; dies gilt insbesondere für Auskünfte über Unternehmen sowie deren Geschäftsbeziehungen oder Kostenelemente.

(73) Damit die ENISA ihre Ziele in vollem Umfang verwirklichen kann, sollte sie mit den einschlägigen Aufsichtsbehörden und anderen zuständigen Behörden in der Union sowie relevanten Einrichtungen der Union zusammenarbeiten – etwa mit dem CERT-EU, EC3 bei Europol, dem ECCC, der Europäischen Verteidigungsagentur (EDA), der Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), dem Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK), der Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), der Europäischen Zentralbank (EZB), der Europäischen Bankenaufsichtsbehörde (EBA), dem Europäischen Datenschutzausschuss, der Agentur für die Zusammenarbeit der

---

54 Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43, ELI: http://data.europa.eu/eli/reg/2001/1049/oj).

55 Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Energieregulierungsbehörden (ACER), der Europäischen Agentur für Flugsicherheit (EASA) und sonstigen Einrichtungen der Union, die sich mit Fragen der Cybersicherheit beschäftigen. Die ENISA sollte mit zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555, Marktüberwachungsbehörden und Datenschutzbehörden zusammenarbeiten, um Know-how und bewährte Verfahren auszutauschen und in Fragen der Cybersicherheit zu beraten, die sich auf die Arbeit der genannten Behörden auswirken können.

(74) Europol spielt eine wichtige Rolle bei der Verhinderung und Bekämpfung von Cyberkriminalität, auch Cyberkriminalität im Zusammenhang mit Netz- und Informationssicherheitsvorfällen. Um Synergien zwischen den jeweiligen Aufgaben der Agenturen zu schaffen, sollte die ENISA mit Europol zusammenarbeiten, insbesondere durch den Austausch von Informationen über Trends bei Techniken, Forderungen und Auswirkungen von Ransomware-Angriffen. Eine solche Zusammenarbeit kann auch darin bestehen, die häufigsten Arten von Ransomware-Angriffen zu ermitteln, die sich gegen in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführte Einrichtungen richten, um wesentliche und wichtige Einrichtungen bei der Reaktion auf Sicherheitsvorfälle und der Wiederherstellung danach zu unterstützen.

(75) Zur Unterstützung der operativen Zusammenarbeit und der gemeinsamen Lageerfassung bei Cyberbedrohungen und -vorfällen ist es von wesentlicher Bedeutung, dass die ENISA mit Interessenträgern und insbesondere Unternehmen und Organisationen aus dem Privatsektor zusammenarbeitet, mit denen die ENISA öffentlich-private Partnerschaften eingehen kann.

(76) Um die in dieser Verordnung dargelegten Ziele wirksam zu erreichen, kann die ENISA insbesondere mit akademischen Einrichtungen zusammenarbeiten, die Forschungsinitiativen in einschlägigen Bereichen betreiben, und geeignete Kanäle für Beiträge von Verbraucherschutzverbänden und anderen Organisationen aufbauen.

(77) Da Cyberbedrohungen und -vorfälle nicht an Grenzen haltmachen, kann sich das Cybersicherheitsniveau und die Abwehrbereitschaft von Drittländern auf Einrichtungen in der Union auswirken. Deshalb sollte die ENISA in der Lage sein, im Einklang mit den Prioritäten der Union Maßnahmen zum Kapazitätsaufbau durchzuführen, einschließlich Schulungen, Partnerschaftsaktivitäten in Drittländern und insbesondere maßgeschneiderter Maßnahmen zum Kapazitätsaufbau für Länder, die Kandidaten für den Beitritt zur Union sind, oder andere Partnerländer. Diese Maßnahmen sollten unter Berücksichtigung der Prioritäten der Union auf ein konkretes Ersuchen um angemessene Unterstützung hin und im Wege von Sonderregelungen, einschließlich Beitragsvereinbarungen gemäß der Verordnung (EU, Euratom) 2024/2509, durchgeführt werden. Der europäische Rahmen für die Cybersicherheitszertifizierung soll vor Cyberbedrohungen wie böswillig ausgenutzten Cybersicherheitsschwachstellen oder Cybersicherheitsvorfällen schützen, die die Funktionalität (Konzeption und Betrieb) von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder die Cyberabwehr von Einrichtungen beeinträchtigen. Indem der Schwerpunkt auf technische Risiken im Zusammenhang mit IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen gelegt wird, sollte der ECCF den Rahmen für die Sicherheit der IKT-Lieferketten ergänzen, mit dem ein harmonisierter Ansatz auf Unionsebene zur Bewältigung nicht technischer Risiken in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren sichergestellt werden soll.

(78) Den Mitgliedstaaten sollte es möglich sein, im Zusammenhang mit öffentlichen Ausschreibungen gemäß der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates[56] auf eine europäische Cybersicherheitszertifizierung zurückgreifen.

(79) Um den Einrichtungen die Einhaltung der Vorschriften zu erleichtern, sollte der ECCF die Möglichkeit vorsehen, ihre Cyberabwehr zu zertifizieren. Einrichtungen, insbesondere solche, die mehrere Arten von Diensten in mehreren Mitgliedstaaten erbringen, können im Rahmen horizontaler Instrumente wie der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[57] und der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[58] sowie sektorspezifischer Instrumente mit unterschiedlichen Verpflichtungen in Bezug auf Cybersicherheit und Datensicherheit konfrontiert sein. Um die Umsetzung des allgemeinen Regelungsrahmens für die Cybersicherheit zu straffen und dessen Einhaltung zu erleichtern, sollten die Rechtsvorschriften der Union die Möglichkeit zulassen, dass Einrichtungen die Einhaltung der Anforderungen an das Risikomanagement im Bereich der Cybersicherheit durch ein europäisches Cybersicherheitszertifikat nachweisen können. Ein einschlägiges System könnte dazu beitragen, die Einhaltungsanforderungen, die sich aus verschiedenen Regulierungsinstrumenten ergeben, unbeschadet ihrer spezifischen Zertifizierungsanforderungen zu straffen. Mit solchen Vereinfachungsmaßnahmen lassen sich der Verwaltungsaufwand verringern und Ressourcen freisetzen, um die operative Abwehrbereitschaft im Bereich der Cybersicherheit von Einrichtungen in kritischen Sektoren der Union zu stärken.

(80) Die europäische Zertifizierung der im Rahmen des ECCF ausgearbeiteten Anforderungen an das Risikomanagement im Bereich der Cybersicherheit sollte es Einrichtungen ermöglichen, die Einhaltung der einschlägigen Rechtsvorschriften der Union nachzuweisen, wenn ein System die entsprechenden in einer solchen Rechtsvorschrift festgelegten rechtlichen Anforderungen abdeckt und wenn dies in diesem System vorgesehen ist. Auf dieser Grundlage kann ein Rechtsakt der Union auch eine Vermutung der Konformität mit diesen Anforderungen vorsehen. Solche Systeme könnten dazu beitragen, die kohärente Umsetzung der in den Rechtsvorschriften der Union enthaltenen Cybersicherheitsanforderungen zu verbessern, um gleiche Wettbewerbsbedingungen in allen Mitgliedstaaten zu schaffen und den Befolgungsaufwand zu verringern.

(81) Durch den europäischen Rahmen für die Cybersicherheitszertifizierung sollten IKT-Prozesse zertifiziert werden können, die als jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll,

---

56 Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

57 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj). http://data.europa.eu/eli/reg/2016/679/oj).

58 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

definiert sind. Ein Schutzprofil ist ein Beispiel für einen IKT-Prozess gemäß der Durchführungsverordnung (EU) 2024/482 der Kommission[59]. Ein weiteres Beispiel für einen IKT-Prozess ist jegliche Tätigkeit eines Herstellers zur sicheren Konzeption und Entwicklung eines IKT-Produkts, einschließlich der physischen, logischen, verfahrenstechnischen, personellen und sonstigen Sicherheitsmaßnahmen, die erforderlich sind, um die Vertraulichkeit und Integrität der Konzeption und der Umsetzung eines IKT-Produkts in seiner Entwicklungsumgebung zu schützen. Die Zertifizierung solcher Tätigkeiten wird häufig als „Standortzertifizierung“ im Rahmen eines Zertifizierungsverfahrens gemäß der Durchführungsverordnung (EU) 2024/482 der Kommission bezeichnet.

(82) Die Begriffsbestimmung für verwaltete Sicherheitsdienste in dieser Verordnung sollte mit der Begriffsbestimmung für Anbieter verwalteter Sicherheitsdienste in der Richtlinie (EU) 2022/2555 im Einklang stehen. Diese Dienste bestehen in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement ihrer Kunden und haben bei der Verhütung und Eindämmung von Vorfällen an Bedeutung gewonnen. Dementsprechend gelten die Anbieter dieser Dienste gemäß der Richtlinie (EU) 2022/2555 als wesentliche oder wichtige Einrichtungen, die zu einem Sektor mit hoher Kritikalität gehören. Anbieter verwalteter Sicherheitsdienste spielen in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen sowie die Wiederherstellung danach unterstützen. Anbieter verwalteter Sicherheitsdienste sind jedoch auch selbst Ziel von Cyberangriffen geworden und stellen aufgrund ihrer engen Einbindung in die Betriebstätigkeit ihrer Kunden ein besonderes Risiko dar. Es ist daher erforderlich, dass wesentliche und wichtige Einrichtungen im Sinne der Richtlinie (EU) 2022/2555 bei der Wahl von Anbietern verwalteter Sicherheitsdienste erhöhte Sorgfalt walten lassen.

(83) Europäische Systeme für die Cybersicherheitszertifizierung sind für ein breites Spektrum von Interessenträgern relevant, so z. B. für Anbieter von IKT-Lösungen, Konformitätsbewertungsstellen und Nutzer. Um eine breite Einbeziehung der Interessenträger zu fördern, sollte die europäische Versammlung für die Cybersicherheitszertifizierung (im Folgenden „Versammlung“) mindestens einmal jährlich abgehalten werden, um die Zusammenarbeit zwischen der Kommission, der ENISA, den Mitgliedstaaten und den einschlägigen Interessenträgern zu fördern. Sie wird eine zentrale Rolle bei der Ermittlung und Bewältigung neuer Herausforderungen im Bereich der Cybersicherheit und strategischer Prioritäten im Bereich der Zertifizierung spielen und sicherstellen, dass Zertifizierungssysteme die sichere Integration digitaler Technologien erleichtern und den Bedürfnissen der Nutzer gerecht werden. Die Versammlung sollte die Führungsrolle der Union bei Zertifizierungstätigkeiten stärken und weiterhin dafür sorgen, dass durch den Zertifizierungsrahmen Vertrauen bei Unternehmen, Behörden und der Öffentlichkeit entsteht.

---

[59] Durchführungsverordnung (EU) 2024/482 der Kommission vom 31. Januar 2024 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC) (ABl. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj). http://data.europa.eu/eli/reg_impl/2024/482/oj).

(84) Die Kommission sollte eine eigene Website unterhalten, um Transparenz zu gewährleisten, indem sie aktuelle Informationen über die Fortschritte bei der Umsetzung des ECCF veröffentlicht. Die Website sollte Informationen über Zertifizierungssysteme, die sich in der Ausarbeitung befinden, strategische Prioritäten für künftige Zertifizierungssysteme, an die ENISA gerichtete Aufträge zur Ausarbeitung möglicher Zertifizierungssysteme und Informationen über die Annahme von Zertifizierungssystemen enthalten. Die Website der Kommission wird die ENISA-Website zu europäischen Systemen für die Cybersicherheitszertifizierung ergänzen, die umfassende Einzelheiten zur technischen Ausarbeitung möglicher Systeme und zur Pflege der Systeme enthalten sollte, wobei der Schwerpunkt auf ausgestellten europäischen Cybersicherheitszertifikaten und EU-Konformitätserklärungen liegen sollte.

(85) Um den Dialog zwischen den Organen der Union zu fördern und zu einem förmlichen, offenen, transparenten und inklusiven Konsultationsprozess beizutragen, sollte die Kommission bei der Bewertung dieser Verordnung Elemente berücksichtigen, die sich aus den Standpunkten des Europäischen Parlaments, des Rates und der europäischen Versammlung für die Cybersicherheitszertifizierung ergeben.

(86) Die von der ENISA vorgenommenen Durchführbarkeitsstudien sollten zur Vorbereitung der Ausarbeitung und Entwicklung von Systemen für die Cybersicherheitszertifizierung beitragen. Die Studien sollten die Perspektiven der einschlägigen Interessenträger berücksichtigen und dafür sorgen, dass die künftigen Zertifizierungssysteme laufenden Forschungs-, Entwicklungs- und technologischen Bewertungstätigkeiten entsprechen, wobei insbesondere die Beiträge von Forschungsinitiativen der Union und der Mitgliedstaaten einfließen sollten. Solche Studien können dazu beitragen, verfügbare Normen und technische Spezifikationen zu ermitteln. Sie sollten im Auftrag der Kommission oder im Einklang mit den strategischen Prioritäten der Union durchgeführt werden, um sicherzustellen, dass der technologischen Entwicklung und dem sich wandelnden Cybersicherheitsbedarf bei der Inauftraggabe und Entwicklung von Systemen angemessen Rechnung getragen wird.

(87) Wie das mögliche System konzipiert wird und welche Sicherheitsziele und -elemente es abdeckt, sollte sich nach Gegenstand und Umfang des Zertifizierungsobjekts richten. So könnte beispielsweise ein Zertifizierungssystem für Cloud-Dienste Sicherheitsziele abdecken, die für IKT-Dienste und die organisatorische Sicherheit relevant sind. Als weiteres Beispiel dürfte ein Sicherheitsziel im Zusammenhang mit der Nichteinbeziehung bekannter ausnutzbarer Schwachstellen für die Zertifizierung von IKT-Prozessen wahrscheinlich nicht relevant sein.

(88) Um sicherzustellen, dass die europäischen Systeme für die Cybersicherheitszertifizierung in allen Mitgliedstaaten einheitlich umgesetzt werden, müssen Vorschriften für die Pflege der Systeme festgelegt werden. Systempflegetätigkeiten sind auch erforderlich, um sicherzustellen, dass die Systeme und ihre Begleitunterlagen auf dem neuesten Stand bleiben, insbesondere im Bereich der Cybersicherheit, in dem sich die Bedrohungslage und die Technologien ständig weiterentwickeln. Zertifizierungssysteme sollten daher so konzipiert und gepflegt werden, dass das Risiko eines schnellen Veraltens vermieden wird. Die Systempflegetätigkeiten sollten in der Regel die Erstellung und Aktualisierung von Begleitunterlagen, einschließlich technischer Spezifikationen und Leitlinien, sowie die Ermittlung von Normen oder technischen Spezifikationen umfassen, die für das System relevant sind. Auch die Analyse der Funktionsweise des Systems, seiner

potenziellen Mängel und der erforderlichen Verbesserungen sollte Teil der Systempflegetätigkeiten sein. Darüber hinaus sollten die Systempflegetätigkeiten die Informationsweitergabe zwischen den Mitgliedstaaten über die Umsetzung der Systeme und Beiträge zu den Mechanismen für die gegenseitige Begutachtung und die gegenseitige Bewertung umfassen.

(89) Aufgrund des technischen Charakters der Systempflegetätigkeiten sollte die ENISA diese in Zusammenarbeit mit der Kommission und mit Unterstützung der Europäischen Gruppe für die Cybersicherheitszertifizierung (ECCG) und ihrer einschlägigen für die Systempflege zuständigen Untergruppe steuern. Durch die Einrichtung der für die Systempflege zuständigen ECCG-Untergruppe können technische Beiträge und Erkenntnisse aus den Mitgliedstaaten zusammengetragen werden, um die Ansätze zu harmonisieren.

(90) Die Systempflegetätigkeiten sollten Interaktionen mit einschlägigen Interessengruppen umfassen, um sicherzustellen, dass die Systeme marktrelevant und auf dem neuesten Stand bleiben, unter anderem durch die gemeinsame Nutzung und die Einholung technischer Beiträge. Bei diesen Interessengruppen kann es sich um Normungsorganisationen, Konformitätsbewertungsstellen, Anbieter, Nutzer, Behörden oder Wirtschaftsverbände handeln. Aufgrund der Besonderheiten jedes Systems, einschließlich der entsprechenden technischen Foren und Branchen, sollte es möglich sein, technische Beiträge je nach System auf unterschiedliche Weise einzuholen. Bei manchen Systemen sollte die ENISA auf eine Ad-hoc-Arbeitsgruppe zurückgreifen können, in der Sachverständige aus den öffentlichen Verwaltungen der Mitgliedstaaten, Einrichtungen der Union und dem Privatsektor vertreten sind. Technische Beiträge könnten auch von Informationsaustausch- und -analysezentren oder Normungsorganisationen geleistet werden. Die ENISA sollte analysieren, welches Format sich für das jeweilige System am besten eignet, und in jedes mögliche System eine Systempflegestrategie aufnehmen.

(91) Die europäischen Systeme für die Cybersicherheitszertifizierung sollten insbesondere bei der Festlegung von Sicherheitsanforderungen und Bewertungsmethoden auf Normen oder technischen Spezifikationen beruhen. Die ENISA sollte die Möglichkeit erhalten, technische Spezifikationen zu erstellen, um die Ausarbeitung und Pflege von Systemen zu unterstützen, insbesondere wenn Dokumente von Normungsorganisationen fehlen oder nicht geeignet sind, die Ziele des Systems zu erreichen. Im Rahmen der Ausarbeitung sollte die ENISA von der ECCG und gegebenenfalls von der für das betreffende System eingerichteten Ad-hoc-Arbeitsgruppe unterstützt werden. Die ENISA sollte auch Beiträge von Interessengruppen einholen. Darüber hinaus sollte die ENISA die Marktakzeptanz sowie europäische und internationale Normen berücksichtigen. Unter Berücksichtigung der Qualität der technischen Spezifikationen und der Ziele des Systems sollte die Kommission in einem europäischen System für die Cybersicherheitszertifizierung auf von der ENISA ausgearbeitete technische Spezifikationen Bezug nehmen können.

(92) Die von der ENISA ausgearbeiteten technischen Spezifikationen, auf die in einem System Bezug genommen wird, sollten auf der ENISA-Website zu europäischen Systemen für die Cybersicherheitszertifizierung veröffentlicht werden, damit alle interessierten Kreise darauf zugreifen können. In einigen spezifischen Fällen könnte die Veröffentlichung auf der Website jedoch ein Risiko für die Cybersicherheit zertifizierter IKT-Produkte, -Dienste und -Prozesse, verwalteter Sicherheitsdienste oder der Cyberabwehr von Einrichtungen und damit auch für die öffentliche Sicherheit

darstellen. Beispielsweise könnten technische Spezifikationen genaue Informationen über neue Angriffswege enthalten, deren öffentliche Verfügbarkeit es böswilligen Akteuren ermöglichen würde, sie auszunutzen. Diese Art von Informationen sollte in begrenztem Umfang nach dem Grundsatz „Kenntnis nur, wenn nötig“ an einschlägige Interessenträger wie nationale Behörden für die Cybersicherheitszertifizierung, Konformitätsbewertungsstellen und zertifizierte Anbieter weitergegeben werden. Aufgrund ihrer eingeschränkten Verbreitung sollte in den europäischen Systemen für die Cybersicherheitszertifizierung nicht auf solche technischen Spezifikationen Bezug genommen werden, weshalb sie nicht verbindlich sein sollten.

(93) Die Systeme für die Zertifizierung der Cyberabwehr sollten modular konzipiert werden, um den Nachweis und die Vermutung der Konformität mit den in anderen Rechtsvorschriften der Union festgelegten einschlägigen Cybersicherheitsanforderungen zu ermöglichen, sofern diese Möglichkeit in diesen Rechtsvorschriften vorgesehen ist. Die Vermutung der Konformität mit den Anforderungen dieser Rechtsakte gilt daher nur dann als Möglichkeit zum Nachweis der Konformität, wenn die entsprechenden Rechtsakte eine solche Konformitätsvermutung zulassen. Die einzelnen Aspekte eines solchen Systems, d. h. Zweck, Ziele oder Elemente, werden sich daher wahrscheinlich von denen anderer Systeme unterscheiden. Systeme für die Zertifizierung der Cyberabwehr von Einrichtungen sollten insbesondere entwickelt werden, um zu bewerten, ob eine Einrichtung die Rechtsvorschriften der Union kontinuierlich einhält. Daher müssen Systeme für die Zertifizierung der Cyberabwehr nicht alle Elemente der europäischen Systeme für die Cybersicherheitszertifizierung, wie z. B. Vertrauenswürdigkeitsstufen, abdecken, was sich in den Vorschriften für die Systeme widerspiegeln sollte.

(94) Durch einen Rahmen für die Zertifizierung der Cyberabwehr innerhalb des ECCF kann ein System entwickelt werden, über das Einrichtungen, die Dienste in mehreren Mitgliedstaaten erbringen, die Einhaltung der in der Richtlinie 2022/2555 des Europäischen Parlaments und des Rates festgelegten Verpflichtungen zum Cybersicherheitsrisikomanagement nachweisen können. Auf dieser Grundlage können Einrichtungen, die die Einhaltung der Vorschriften nachweisen können, von kohärenteren und weniger aufwendigen Aufsichtskonzepten im gesamten Binnenmarkt profitieren. Die Entwicklung eines solchen Zertifizierungssystems sollte durch den Erlass von Durchführungsrechtsakten gemäß der Richtlinie (EU) 2022/2555 erleichtert werden. Durch Erweiterungsprofile kann mithilfe eines Systems zur Zertifizierung der Cyberabwehr die Einhaltung der Anforderungen nachgewiesen werden, wenn ein Mitgliedstaat Bestimmungen erlassen oder beibehalten hat, die ein höheres Maß an Cybersicherheit im Einklang mit der Richtlinie (EU) 2022/2555 gewährleisten. Auf dieser Grundlage kann eine Einrichtung, die Dienste in mehreren Mitgliedstaaten erbringt, die Einhaltung aller einschlägigen Erweiterungsprofile durch ein einziges europäisches Cybersicherheitszertifikat nachweisen.

(95) Die Sicherheitsziele und Sicherheitsanforderungen, die in den europäischen Systemen für die Cybersicherheitszertifizierung in Bezug auf die Produktsicherheit festgelegt sind, sollten mit den grundlegenden Cybersicherheitsanforderungen in Anhang I der Verordnung (EU) 2024/2847 im Einklang stehen. Diese Kohärenz ist erforderlich, um sicherzustellen, dass Hersteller, deren Produkte in den Anwendungsbereich der Verordnung (EU) 2024/2847 fallen, bei der Zertifizierung ihrer Produkte im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung keinen widersprüchlichen Anforderungen unterliegen. Darüber hinaus erleichtert die Kohärenz der Anforderungen die Konformitätsvermutung gemäß Artikel 27 der

Verordnung (EU) 2024/2847, wonach bei Herstellern von Produkten mit digitalen Elementen, die im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung zertifiziert wurden, unter bestimmten Bedingungen die Konformität mit den grundlegenden Cybersicherheitsanforderungen in Anhang I der genannten Verordnung vermutet wird.

(96) Im Rahmen des europäischen Systems für die Cybersicherheitszertifizierung sollte es möglich sein, ein Erweiterungsprofil festzulegen, indem zusätzliche oder spezifische Anforderungen für Anwendungsfälle festgelegt werden, einschließlich zusätzlicher Fähigkeiten wie verbesserter Produktmerkmale, spezialisierter Dienstangebote oder Assets, optimierter Prozesse und fortgeschrittener Sicherheitsmaßnahmen. Da Erweiterungsprofile keiner bestimmten Vertrauenswürdigkeitsstufe entsprechen, sollte ihr Zweck, einschließlich der behandelten Sicherheitsbedrohungen, detailliert beschrieben werden. Erweiterungsprofile dienen insbesondere dazu, die Einhaltung bestimmter Normen und Regulierungsanforderungen nachzuweisen, gegebenenfalls einschließlich Anforderungen in Bezug auf zusätzliche Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die von einem Mitgliedstaat nach dem Grundsatz der Mindestharmonisierung im Einklang mit der Richtlinie (EU) 2022/2555 festgelegt wurden.

(97) Unbeschadet des allgemeinen Systems der gegenseitigen Begutachtung, das alle nationalen Behörden für die Cybersicherheitszertifizierung im Rahmen des ECCF einrichten müssen, sollte es möglich sein, in die europäischen Systeme für die Cybersicherheitszertifizierung einen Mechanismus zur gegenseitigen Bewertung für die Stellen aufzunehmen, die europäische Cybersicherheitszertifikate für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und die Cyberabwehr von Einrichtungen ausstellen, insbesondere für Stellen, die im Rahmen solcher Systeme Zertifikate mit der Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Diese Stellen sollten auch Zertifizierungsstellen der nationalen Behörden für die Cybersicherheitszertifizierung einschließen, die Zertifikate der Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Die ECCG sollte die Umsetzung der Verfahren der gegenseitigen Bewertung unterstützen. Bei solchen gegenseitigen Bewertungen sollte insbesondere beurteilt werden, ob die betreffenden Stellen ihre Aufgaben einheitlich ausführen; zudem können sie Einspruchsmöglichkeiten umfassen.

(98) Krisen wie Kriege, Naturkatastrophen und Pandemien könnten sich negativ auf Zertifizierungstätigkeiten auswirken. In Krisenszenarien dieser Art kann es sein, dass sich beispielsweise die Sicherheit des Standorts aufgrund zerstörter Infrastruktur, wegen Cyberangriffen, der Nichtverfügbarkeit von Personal und der Unzugänglichkeit des Standorts nicht gewährleisten lässt. In einem europäischen System für die Cybersicherheitszertifizierung sollten daher befristete Vorschriften für die Aufrechterhaltung von Zertifizierungstätigkeiten in solchen Szenarien festgelegt werden.

(99) Die Umsetzung möglicher technischer Systeme in Durchführungsrechtsakte erfordert umfassende technische und rechtliche Fachkenntnisse und kann erheblichen Verwaltungsaufwand verursachen. Darüber hinaus sind bestimmte Elemente europäischer Systeme für die Cybersicherheitszertifizierung, wie das Schwachstellenmanagement oder die Bedingungen, unter denen solche Siegel oder Kennzeichen verwendet werden dürfen, sektorübergreifend, weshalb harmonisierte Referenzbestimmungen von Vorteil wären. Um die Qualität angenommener europäischer Systeme für die Cybersicherheitszertifizierung zu gewährleisten und den

Befolgungsaufwand für Unternehmen zu verringern, sollte der Kommission die Befugnis übertragen werden, Mustervorschriften für bestimmte Elemente der europäischen Systeme für die Cybersicherheitszertifizierung zu erlassen.

(100) Um die Kohärenz des europäischen Rahmens für die Cybersicherheitszertifizierung zu gewährleisten, sollte es innerhalb eines europäischen Systems für die Cybersicherheitszertifizierung möglich sein, die Vertrauenswürdigkeitsstufen für europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, die im Rahmen dieses Systems ausgestellt werden, anzugeben. Ein europäisches Cybersicherheitszertifikat sollte sich auf eine der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ beziehen, wohingegen sich die EU-Konformitätserklärung nur auf die Vertrauenswürdigkeitsstufe „niedrig“ beziehen sollte. Die Vertrauenswürdigkeitsstufen sollten die entsprechende Strenge und Gründlichkeit für die Bewertung des IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder der Cyberabwehr einer Einrichtung vorgeben und durch Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren, einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Vorfällen besteht, gekennzeichnet sein. Jede Vertrauenswürdigkeitsstufe sollte in den verschiedenen Bereichen der Sektoren, in denen die Zertifizierung angewandt wird, einheitlich sein.

(101) Die Auswahl der angemessenen Zertifizierung und der dazugehörigen Sicherheitsanforderungen durch die Nutzer der europäischen Cybersicherheitszertifikate sollte auf der Grundlage einer Risikoanalyse der Verwendung des IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder des Zertifizierungskontexts von Einrichtungen erfolgen. Dementsprechend sollte die Vertrauenswürdigkeitsstufe in einem angemessenen Verhältnis zu dem Risiko stehen, das mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses, der verwalteten Sicherheitsdienste oder mit der Betriebsumgebung und der Art der Einrichtung verbunden ist, deren Cyberabwehr Gegenstand einer Zertifizierung ist.

(102) Bei der Vertrauenswürdigkeitsstufe „niedrig“ sollte sich die Bewertung mindestens auf die folgenden Vertrauenswürdigkeitskomponenten stützen: Die Bewertung sollte mindestens eine Überprüfung der technischen Dokumentation des IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder der Cyberabwehr einer Einrichtung durch die Konformitätsbewertungsstelle umfassen. Schließt die Zertifizierung IKT-Prozesse ein, sollte auch das Verfahren zur Konzipierung, Entwicklung und Pflege eines IKT-Produkts oder -Dienstes, eines verwalteten Sicherheitsdienstes oder der Cyberabwehr einer Einrichtung einer technischen Überprüfung unterzogen werden. Sieht ein europäisches System für die Cybersicherheitszertifizierung eine Selbstbewertung der Konformität vor, so sollte es ausreichen, dass der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder die Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist, eine Selbstbewertung der Konformität des IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder der Cyberabwehr dieser Einrichtung mit dem Zertifizierungssystem vorgenommen hat.

(103) Bei der Vertrauenswürdigkeitsstufe „mittel“ sollte sich die Bewertung – zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „niedrig“ – mindestens auf eine Überprüfung der Konformität der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder der Cyberabwehr einer Einrichtung mit ihrer technischen Dokumentation stützen.

(104) Bei der Vertrauenswürdigkeitsstufe „hoch“ sollte sich die Bewertung – zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „mittel“ – mindestens auf einen Wirksamkeitstest stützen, bei dem die Widerstandsfähigkeit der Sicherheitsfunktionen gegen gründlich vorbereitete Cyberattacken bewertet wird, die von Akteuren mit umfangreichen Fähigkeiten und Ressourcen durchgeführt werden. Für die Vertrauenswürdigkeitsstufe „hoch“ oder in den Fällen, in denen ein System so ausgelegt ist, dass die Konformität nachgewiesen wird und eine Konformitätsvermutung mit anderen Rechtsvorschriften der Union vorliegt, sollten die Konformitätsbewertungstätigkeiten im Europäischen Wirtschaftsraum durchgeführt werden. Diese Anforderung ist dadurch gerechtfertigt, dass Bewertungstätigkeiten außerhalb des Europäischen Wirtschaftsraums zusätzliche Bedrohungen für die Cybersicherheit darstellen, insbesondere bezüglich des geistigen Eigentums der bewerteten IKT-Produkte, -Dienste oder -Prozesse, der verwalteten Sicherheitsdienste oder der Einrichtungen. So könnte beispielsweise der Quellcode eines IKT-Produkts bei Nutzung in einem Drittland ausgelesen werden, was ein Risiko für das geistige Eigentum darstellt. Darüber hinaus sind in Drittländern niedergelassene Prüflabors nicht in einer Umgebung tätig, die den durch EU-Rechtsvorschriften wie die Richtlinie (EU) 2022/2555 oder die Verordnung (EU) 2024/2847 festgelegten Cybersicherheitsmaßnahmen unterliegen. So kann ein Prüflabor beispielsweise auf einen Cloud-Dienstanbieter aus einem Drittland zurückgreifen, der die Cybersicherheitsanforderungen der Richtlinie (EU) 2022/2555 nicht einhält. Dennoch sollte es zulässig sein, in einem Zertifizierungssystem Ausnahmeregelungen vorzusehen, beispielsweise im Zusammenhang mit der Standortzertifizierung oder in anderen Fällen, in denen Konformitätsbewertungstätigkeiten im Europäischen Wirtschaftsraum nicht angemessen durchgeführt werden können.

(105) In manchen Fällen können unterschiedliche Ansätze erforderlich sein, um die Sicherheitsziele einer bestimmten Vertrauenswürdigkeitsstufe zu erreichen und dabei den Besonderheiten eines IKT-Produkts, -Dienstes oder -Prozesses, verwalteter Sicherheitsdienste oder der Cyberabwehr von Einrichtungen Rechnung zu tragen. Um ein kleinteiligeres Vorgehen zu ermöglichen, sollte es in einem europäischen System für die Cybersicherheitszertifizierung möglich sein, ein oder mehrere Bewertungsniveaus festzulegen, die einer der Vertrauenswürdigkeitsstufen entsprechen. Dies wird die Entwicklung von Systemen ermöglichen, bei denen mehrere, für einen anderen Zweck konzipierte Bewertungsniveaus der mit einem bestimmten Sicherheitsniveau verbundenen Vertrauenswürdigkeitsstufe entsprechen.

(106) Es sollte zulässig sein, dass europäische Systeme für die Cybersicherheitszertifizierung die Durchführung einer Konformitätsbewertung unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder von Einrichtungen, deren Cyberabwehr zertifiziert wird, vorsehen (Selbstbewertung der Konformität). In solchen Fällen sollte es ausreichen, dass der Hersteller, der Anbieter oder die Einrichtung, deren Cyberabwehr zertifiziert wird, alle Kontrollen selbst durchführt, durch die sichergestellt wird, dass die IKT-Produkte, -Dienste und -Prozesse, der verwaltete Sicherheitsdienst oder die Cyberabwehr einer Einrichtung dem europäischen System für die Cybersicherheitszertifizierung entsprechen. Die Selbstbewertung der Konformität sollte bei IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen als angemessen gelten, die von geringer Komplexität sind, ein geringes Risiko für die Öffentlichkeit darstellen und eine einfache Konzeption und einfache Herstellungsmechanismen aufweisen.

(107) Sind in einem europäischen System für die Cybersicherheitszertifizierung sowohl Selbstbewertungen der Konformität als auch Zertifizierungen von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen möglich, sollten im Zertifizierungssystem klare und verständliche Instrumente für Verbraucher oder andere Nutzer vorgesehen werden, mit denen sie zwischen IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen, die selbst bewertet wurden, und solchen, die durch Dritte zertifiziert wurden, unterscheiden können.

(108) Die Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten bzw. die Einrichtungen, deren Cyberabwehr zertifiziert wird, sollten die EU-Konformitätserklärung im Rahmen des Konformitätsbewertungsverfahrens ausstellen und unterzeichnen können. Eine EU-Konformitätserklärung ist ein Dokument, welches bestätigt, dass das betreffende IKT-Produkt bzw. der betreffende IKT-Dienst oder -Prozess, der betreffende verwaltete Sicherheitsdienst oder die Cyberabwehr der betreffenden Einrichtung die Anforderungen des europäischen Systems für die Cybersicherheitszertifizierung erfüllt. Durch die Ausstellung und Unterzeichnung der EU-Konformitätserklärung übernimmt der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder die Einrichtung, deren Cyberabwehr zertifiziert wird, die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, der verwaltete Sicherheitsdienst oder die Cyberabwehr der Einrichtung den Anforderungen des europäischen Systems für die Cybersicherheitszertifizierung entspricht. Eine Kopie der EU-Konformitätserklärung sollte der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorgelegt werden.

(109) Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder Einrichtungen, deren Cyberabwehr zertifiziert wird, sollten der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung im Einklang mit den geltenden Rechtsvorschriften der Union die EU-Konformitätserklärung, die technische Dokumentation und alle anderen relevanten Informationen im Zusammenhang mit der Konformität mit einem europäischen System für die Cybersicherheitszertifizierung für einen im entsprechenden europäischen System für die Cybersicherheitszertifizierung vorgesehenen Zeitraum zur Verfügung stellen. In der technischen Dokumentation sollten die im Rahmen des Systems geltenden Anforderungen angegeben werden, soweit sie für die Selbstbewertung der Konformität relevant sind. Die technische Dokumentation sollte so erstellt werden, dass bewertet werden kann, ob ein IKT-Produkt, ein IKT-Dienst, ein IKT-Prozess, ein verwalteter Sicherheitsdienst oder die Cyberabwehr der Einrichtung die im Rahmen des Systems geltenden Anforderungen erfüllt.

(110) Die europäischen Cybersicherheitszertifikate und die EU-Konformitätserklärung sollten den Nutzern dabei helfen, kundige Entscheidungen zu treffen. Daher sollten einschlägige Informationen auf einer von der ENISA betriebenen Website veröffentlicht werden. Darüber hinaus sollten IKT-Produkten, -Diensten und -Prozessen, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, strukturierte Informationen beigegeben werden, die an das erwartete technische Niveau des vorgesehenen Nutzers angepasst sind. Alle Nutzer sollten Zugang zu Informationen über die Referenznummer des Zertifizierungssystems, die ausstellende Behörde oder Stelle und gegebenenfalls die Vertrauenswürdigkeitsstufe

haben oder eine Kopie des europäischen Cybersicherheitszertifikats erhalten können. Diese Informationen sollten regelmäßig auf den neuesten Stand gebracht und auf einer eigenen Website über europäische Systeme für die Cybersicherheitszertifizierung zur Verfügung gestellt werden. Um die kontinuierliche Zugänglichkeit zu gewährleisten, sollten Hersteller und Anbieter darüber hinaus verpflichtet sein, die zuständige Zertifizierungsstelle zu unterrichten, wenn sich der Speicherort der Online-Informationen oder gegebenenfalls der Aufbewahrungsort der physischen Informationen ändert.

(111) Eine Konformitätsbewertung ist ein Verfahren, mit dem bewertet wird, ob bestimmte Anforderungen an ein IKT-Produkt, einen IKT-Dienst oder einen IKT-Prozess, einen verwalteten Sicherheitsdienst oder eine Einrichtung erfüllt werden. Dieses Verfahren wird von einem unabhängigen Dritten durchgeführt, bei dem es sich weder um den Hersteller oder Anbieter der zu zertifizierenden IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste noch um die Einrichtung handelt, deren Cyberabwehr bewertet wird. Nach der erfolgreichen Bewertung eines IKT-Produkts, -Dienstes oder -Prozesses, eines verwalteten Sicherheitsdienstes oder der Cyberabwehr der Einrichtung sollte ein europäisches Cybersicherheitszertifikat ausgestellt werden. Dieses sollte als Bestätigung gelten, dass die Bewertung ordnungsgemäß durchgeführt wurde.

(112) Die strikte Trennung der Aufsichts- und Zertifizierungstätigkeiten ist wichtig, um Verzerrungen und Einflussnahmen zu vermeiden, die auftreten können, wenn die den Markt beaufsichtigende Einrichtung auf demselben Markt auch im Wettbewerb steht. Daher sollten Tätigkeiten, bei denen die nationalen Behörden für die Cybersicherheitszertifizierung lediglich ihre Aufsichtsfunktion wahrnehmen, z. B. durch die vorherige Zustimmung zur Ausstellung eines Zertifikats, keine weitere interne Trennung von anderen Aufsichtstätigkeiten erfordern. Hierunter fällt beispielsweise eine Situation, in der die nationale Behörde für die Cybersicherheitszertifizierung während des gesamten Zertifizierungsverfahrens, das von privaten Konformitätsbewertungsstellen durchgeführt wird, aktiv Informationen sammelt und dann ihre Stellungnahme zur Ausstellung des Zertifikats durch diese Stellen abgibt (im Folgenden „Modell der vorherigen Zustimmung“).

(113) In den europäischen Systemen für die Cybersicherheitszertifizierung sollten die Bedingungen festgelegt werden, unter denen IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr einer Einrichtung möglicherweise neu zertifiziert werden müssen oder unter denen der Umfang eines bestimmten europäischen Cybersicherheitszertifikats eingeschränkt werden muss. Darüber hinaus sollten die europäischen Systeme für die Cybersicherheitszertifizierung etwaigen nachteiligen Auswirkungen später festgestellter Schwachstellen oder Unregelmäßigkeiten hinsichtlich des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses, verwalteten Sicherheitsdienstes oder der zertifizierten Cyberabwehr einer Einrichtung im Hinblick auf die Konformität mit den Sicherheitsanforderungen dieses Zertifikats Rechnung tragen.

(114) Harmonisierung spielt eine entscheidende Rolle bei der Gewährleistung einer robusten Cybersicherheit und einem verbesserten Marktzugang für Unternehmen. Im Gegensatz dazu stellen Fragmentierung und fehlende gegenseitige Anerkennung von Zertifikaten erhebliche Hindernisse für den reibungslosen Datenfluss dar, wodurch die Betriebskosten für die Industrie in der Union steigen. Um diesen Herausforderungen zu begegnen, ist es entscheidend, eine Fragmentierung sowohl beim Umfang der

Sicherheitskontrollen als auch bei den Konformitätsbewertungsmethoden in der gesamten Union zu vermeiden.

(115) Die Mitgliedstaaten sollten die Kommission und die ECCG rechtzeitig vor der Annahme neuer nationaler Systeme für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen unterrichten, um die Kommission und die ECCG dabei zu unterstützen, die Auswirkungen des neuen nationalen Systems für die Cybersicherheitszertifizierung auf das ordnungsgemäße Funktionieren des Binnenmarkts zu bewerten, und zwar vor dem Hintergrund eines möglichen strategischen Interesses, ein europäisches System für die Cybersicherheitszertifizierung in Auftrag zu geben.

(116) Verweise im nationalen Recht, die sich auf nationale Normen beziehen, die aufgrund des Inkrafttretens eines europäischen Systems für die Cybersicherheitszertifizierung keine Rechtswirkung mehr haben, können zu Verwirrung führen. Daher sollten die Mitgliedstaaten gegebenenfalls der Annahme eines europäischen Systems für die Cybersicherheitszertifizierung in ihren nationalen Rechtsvorschriften Rechnung tragen.

(117) Um das Wachstum eines verlässlichen Binnenmarkts zu fördern und gleichzeitig Partnerschaften mit Drittländern zu schließen, sollte das im Rahmen des ECCF eingerichtete Zertifizierungsverfahren so umgesetzt werden, dass die internationale Anerkennung, die gegenseitige Anerkennung und die Angleichung an internationale Normen erleichtert werden.

(118) Da die IKT-Lieferketten international sind, kann die Union zur weiteren Erleichterung des Handels gemäß Artikel 218 AEUV Abkommen über die gegenseitige Anerkennung von europäischen Cybersicherheitszertifikaten schließen. Der Kommission sollte die Befugnis übertragen werden, Durchführungsrechtsakte zu erlassen, um die Gleichwertigkeit von in Drittländern ausgestellten Zertifikaten mit europäischen Cybersicherheitszertifikaten einseitig anzuerkennen. Es sollte möglich sein, spezifische Bedingungen für eine solche Anerkennung von in Drittländern ausgestellten Zertifikaten festzulegen.

(119) Zur Erreichung einer gleichwertigen Umsetzung des Rahmens in der gesamten Union, zur Erleichterung der gegenseitigen Anerkennung und zur Förderung der allgemeinen Akzeptanz der europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bedarf es eines Systems der gegenseitigen Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung. Die gegenseitige Begutachtung sollte Verfahren für Folgendes umfassen: Beaufsichtigung der Übereinstimmung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten und der Cyberabwehr von Einrichtungen mit europäischen Cybersicherheitszertifikaten, Überwachung der Verpflichtungen der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten und von zertifizierten Einrichtungen, die eine Selbstbewertung der Konformität vornehmen, Überwachung der Konformitätsbewertungsstellen sowie Angemessenheit der Sachkenntnis des Personals der Einrichtungen, die Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. In Zusammenarbeit mit der Kommission und der ECCG sollte sich die ENISA als Beobachterin an gegenseitigen Begutachtungen beteiligen und die Organisation des Mechanismus der gegenseitigen Begutachtung und der gegenseitigen Begutachtungen selbst, unter anderem durch die Entwicklung einschlägiger Leitlinien und Muster, unterstützen. Die ENISA sollte auf

ihrer Website zu europäischen Systemen für die Cybersicherheitszertifizierung auch den Zeitplan der gegenseitigen Begutachtungen und die Liste der begutachteten nationalen Behörden für die Cybersicherheitszertifizierung, für die dieser Zeitplan gilt, öffentlich zugänglich machen. In der Durchführungsverordnung (EU) 2025/2540 der Kommission[60], die gemäß der Verordnung (EU) 2019/881 erlassen wurde, ist der Plan für die gegenseitige Begutachtung festgelegt, der von den angenommenen europäischen Systemen für die Cybersicherheitszertifizierung verwendet wird. Es muss sichergestellt werden, dass die gegenseitigen Begutachtungen fortgesetzt werden. Dennoch sollte die Kommission im Wege von Durchführungsrechtsakten bei Bedarf einen neuen, mindestens fünfjährigen Plan für die gegenseitige Begutachtung erstellen und Kriterien und Methoden für die Abwicklung der gegenseitigen Begutachtungen festlegen können.

(120) Sobald ein europäisches System für die Cybersicherheitszertifizierung angenommen ist, sollten Hersteller oder Anbieter von IKT-Produkten, -Diensten, -Prozessen, verwalteten Sicherheitsdiensten oder Einrichtungen, deren Cyberabwehr Gegenstand einer Zertifizierung ist, bei der Konformitätsbewertungsstelle ihrer Wahl überall in der Union Anträge auf Zertifizierung ihrer IKT-Produkte, -Dienste oder -Prozesse, verwalteten Sicherheitsdienste oder Cyberabwehr stellen können. Konformitätsbewertungsstellen sollten von einer nationalen Akkreditierungsstelle akkreditiert werden, wenn sie die Anforderungen dieser Verordnung und gegebenenfalls die von der Kommission gemäß dieser Verordnung festgelegten Anforderungen erfüllen. Das in dieser Verordnung vorgesehene System sollte durch das Akkreditierungssystem gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates[61] ergänzt werden.

(121) Konformitätsbewertungsstellen, die nach geltendem Unionsrecht, insbesondere nach der Verordnung (EU) 2024/2847 oder der Durchführungsverordnung (EU) 2024/482, akkreditiert oder notifiziert wurden, verfügen möglicherweise über Kompetenzen, die für neu angenommene europäische Systeme für die Cybersicherheitszertifizierung relevant sind. Um unnötigen finanziellen und administrativen Aufwand zu vermeiden, sollten Synergien für die Akkreditierung von Konformitätsbewertungsstellen im Rahmen dieser Verordnung geschaffen werden. Aus diesem Grund sollten die Akkreditierungsanforderungen in den Systemen so festgelegt werden, dass sie so weit wie möglich den Anforderungen an notifizierte Stellen gemäß der Verordnung (EU) 2024/2847 und den Akkreditierungsanforderungen gemäß der Durchführungsverordnung (EU) 2024/482 entsprechen. Darüber hinaus sollten bei Konformitätsbewertungsstellen, die ein Akkreditierungsverfahren gemäß dieser Verordnung durchlaufen, frühere Ergebnisse der Bewertung ihrer Kompetenzen im Rahmen anderer Rechtsvorschriften der Union herangezogen werden können, wenn sich die Akkreditierungsanforderungen überschneiden.

(122) Um harmonisierte Konformitätsbewertungsdienste in der gesamten Union zu erleichtern, sollten in einem europäischen System für die

---

60 Durchführungsverordnung (EU) 2025/2540 der Kommission vom 9. Dezember 2025 mit Durchführungsbestimmungen zur Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates hinsichtlich der Einrichtung des Plans für die gegenseitige Begutachtung (ABl. L 2540, 12.12.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/2540/oj).

61 Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

Cybersicherheitszertifizierung zusätzliche oder spezifische Anforderungen an Konformitätsbewertungsstellen festgelegt werden können. Im Zusammenhang mit der Zertifizierung sollte eine Zulassung als Entscheidung einer nationalen Behörde für die Cybersicherheitszertifizierung verstanden werden, dass eine Konformitätsbewertungsstelle die in einem europäischen System für die Cybersicherheitszertifizierung festgelegten spezifischen oder zusätzlichen Anforderungen erfüllt, um eine bestimmte Konformitätsbewertungstätigkeit durchzuführen.

(123) Sind in einem europäischen System für die Cybersicherheitszertifizierung zusätzliche oder spezifische Anforderungen gemäß dieser Verordnung festgelegt, so sollte den Konformitätsbewertungsstellen von den benannten nationalen Behörden für die Cybersicherheitszertifizierung die Befugnis erteilt werden, Aufgaben im Rahmen dieses Systems wahrzunehmen. Um Mehrfachzulassungen zu vermeiden, die Akzeptanz und Anerkennung von Zulassungsentscheidungen zu verbessern und befugte Konformitätsbewertungsstellen wirksam zu überwachen, sollten die Konformitätsbewertungsstellen die Zulassung bei der nationalen Behörde für die Cybersicherheitszertifizierung desjenigen Mitgliedstaates beantragen, in dem sie niedergelassen sind. Es muss jedoch sichergestellt werden, dass eine Konformitätsbewertungsstelle in der Lage ist, die Zulassung in einem anderen Mitgliedstaat zu beantragen, falls es in ihrem eigenen Mitgliedstaat keine nationale Behörde für die Cybersicherheitszertifizierung gibt oder falls die nationale Behörde für die Cybersicherheitszertifizierung nicht über die Kompetenz zur Erteilung der verlangten Zulassung verfügt. In solchen Fällen sollten die nationalen Behörden für die Cybersicherheitszertifizierung zusammenarbeiten und Informationen austauschen. Der Kommission sollte die Befugnis übertragen werden, Durchführungsrechtsakte zu erlassen, um die Zulassungsverfahren, auch für die grenzüberschreitende Zusammenarbeit bei der Zulassung, festzulegen.

(124) Zur Wahrung des Schutzniveaus, das für IKT-Produkte, -Dienst oder -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr einer Einrichtung in der Union erforderlich ist, müssen Unterauftragnehmer und Zweigstellen verpflichtet werden, bei der Ausführung der Konformitätsbewertungsaufgaben dieselben Anforderungen zu erfüllen wie die notifizierten Konformitätsbewertungsstellen. Dementsprechend sollte eine Konformitätsbewertungsstelle über die entsprechende Kompetenz verfügen und überprüfen können, ob ihre Unterauftragnehmer die geltenden Anforderungen erfüllen.

(125) Die notifizierende Behörde sollte angemessen beurteilen, inwieweit die Konformitätsbewertungsstelle beabsichtigt, auf außerhalb der Union niedergelassene Unterauftragnehmer zurückzugreifen oder Zugang zu Personal oder Einrichtungen außerhalb des Mitgliedstaats der Notifizierung zu haben. Die Behörde eines Mitgliedstaats sollte entscheiden können, dass sie die Gesamtverantwortung als nationale Behörde für die Cybersicherheitszertifizierung für eine solche Vereinbarung nicht übernehmen kann, und die Notifizierung widerrufen oder deren Umfang einschränken können.

(126) Zur Bewertung der Cybersicherheitsanforderungen für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen sollten die nationalen Behörden für die Cybersicherheitszertifizierung der Kommission und den anderen Mitgliedstaaten akkreditierte Konformitätsbewertungsstellen notifizieren. Die Notifizierung akkreditierter und gegebenenfalls befugter Konformitätsbewertungsstellen bedeutet, dass diesen Stellen bezüglich der Durchführung von Evaluierungs- und Zertifizierungstätigkeiten gemäß dieser

Verordnung und dem europäischen System für die Cybersicherheitszertifizierung vertraut werden kann, was zum guten allgemeinen Ruf der europäischen Cybersicherheitszertifizierung beiträgt. Deshalb muss unbedingt sichergestellt werden, dass die notifizierten Konformitätsbewertungsstellen ihre Anforderungen und Verpflichtungen dauerhaft erfüllen und dass die Liste der notifizierten Konformitätsbewertungsstellen stets aktuell gehalten wird.

(127) In der Durchführungsverordnung (EU) 2024/3143 der Kommission[62], die gemäß der Verordnung (EU) 2019/881 erlassen wurde, sind die Umstände, Formate und Verfahren für die Notifizierung von Konformitätsbewertungsstellen festgelegt, die im Rahmen der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung tätig sind. Daher muss sichergestellt werden, dass die Notifizierungstätigkeiten fortgesetzt werden. Der Kommission sollte jedoch die Befugnis übertragen werden, Durchführungsrechtsakte zu erlassen, um diese Umstände, Verfahren und Formate für die Notifizierung von Konformitätsbewertungsstellen anzupassen. Dabei sollte sich die Kommission auf die im Zusammenhang mit bestehenden Systemen gewonnenen Erfahrungen stützen und eine Angleichung an andere einschlägige Rechtsvorschriften und Rahmen der Union, insbesondere die Verordnung (EU) 2024/2847 und den neuen Rechtsrahmen, anstreben, um den Befolgungsaufwand für Konformitätsbewertungsstellen, die im Rahmen verschiedener Rechtsinstrumente tätig sind, zu verringern.

(128) Die Lieferketten in der Informations- und Kommunikationstechnik (IKT) setzen sich aus einer Reihe miteinander verflochtener Ressourcen und Prozesse zusammen, an denen verschiedene Wirtschaftsteilnehmer mitwirken. IKT-Lieferketten spielen eine wichtige Rolle dabei, die gesellschaftliche Stabilität zu erhalten und die Wirtschaftstätigkeit in der gesamten Union anzukurbeln. Außerdem spielen sie eine entscheidende Rolle, wenn es darum geht, die digitale Infrastruktur in der Union bereitzustellen und das Funktionieren von Wirtschaft und Gesellschaft der Union zu unterstützen. IKT-Lieferketten ermöglichen die Herstellung, die Bereitstellung, den Vertrieb und die Systempflege von IKT-Diensten, -Systemen und -Produkten, die verschiedenen kritischen und hochkritischen Sektoren zugrunde liegen, wie Gesundheitsversorgung, Finanzen, Verkehr, Telekommunikation, Energie und Zoll. Die Sicherheit der IKT-Lieferketten in diesen kritischen Sektoren kann sich auch auf die Sicherheit der Verteidigungs- und militärischen Infrastruktur auswirken, wenn diese Infrastruktur von zivilen kritischen Sektoren und deren IKT-Lieferketten abhängig ist. Dem von der ENISA herausgegebenen Bericht über den Stand der Cybersicherheitsbedrohungen (ENISA Threat Landscape 2025)[63] zufolge gehören Angriffe auf Lieferketten zu den fünf größten Cybersicherheitsbedrohungen, was zeigt, dass Angreifer indirekte Wege über Drittanbieter und Abhängigkeiten aktiv ausnutzen. Die Unterbrechung von IKT-Lieferketten kann die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Daher sind im Bereich der

---

62 Durchführungsverordnung (EU) 2024/3143 der Kommission vom 18. Dezember 2024 zur Festlegung der Umstände, Formate und Verfahren für Notifizierungen nach Artikel 61 Absatz 5 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (ABl. L 3143 vom 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

63 ENISA Threat Landscape 2025, Oktober 2025.

Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.

(129) Neben den technischen Risiken, die in der Richtlinie (EU) 2022/55 des Europäischen Parlaments und des Rates[64], der Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates[65] und dem mit der Verordnung (EU) 2019/881 geschaffenen europäischen Rahmen für die Cybersicherheitszertifizierung behandelt werden, sind IKT-Lieferketten zunehmend nicht technischen Risiken ausgesetzt. Solche nicht technischen Risiken können unter anderem mit der rechtlichen Zuständigkeit zusammenhängen, der ein Anbieter bestimmter Komponenten unterliegt, insbesondere wenn ein Drittland oder ein von diesem Land aus kontrollierter Bedrohungsakteur Wirtschaftsspionage betreibt, böswillige, gegen die Union oder ihre Mitgliedstaaten gerichtete Cyberaktivitäten oder -kampagnen durchführt oder unverantwortliches staatliches Handeln im Cyberraum an den Tag legt. Nicht technische Risiken können auch im Zusammenhang mit versteckten Schwachstellen oder Hintertüren oder potenziellen systemischen Versorgungsunterbrechungen auftreten, insbesondere im Fall von Abhängigkeiten von bestimmten Technologien oder Anbietern. So können beispielsweise Kommunikations- und Stromnetze durch erzwungene Abschaltungen („Kill Switches“) beeinträchtigt werden.

(130) In der Gemeinsamen Mitteilung über die Stärkung der wirtschaftlichen Sicherheit der EU[66] wurde das Risiko betont, dass Drittländer Zugang zu sensiblen Informationen und Daten in der Union oder ihren Mitgliedstaaten erhalten, entweder aufgrund von Industriespionage oder weil sie Hardware oder Software erhalten, die in bestimmten Produkten verwendet wird, oder aber weil sich bestimmte Unternehmen, die im Besitz sensibler Informationen und Daten sind, in ihrem Eigentum oder unter ihrer Kontrolle befinden. Betont wurde in der Mitteilung auch das Risiko von Störungen der kritischen Infrastruktur der Union – einschließlich kritischer Verkehrs-, Weltraum-, Energie- und Kommunikationsinfrastruktur, insbesondere solcher, die von strategischer Bedeutung für die militärische Mobilität ist – durch ausländische Akteure, was zu Kaskadeneffekten auf die Wirtschaft der Union führen könnte. Störungen können durch physische Angriffe, Cyberattacken oder hybride Angriffe auftreten, einschließlich der Sabotage ganzer Anlagen oder ihrer Teile oder Unterkomponenten. Sie könnten auch mit IKT-Lieferketten im Zusammenhang stehen, die die Grundlage für kritische Komponenten oder Dienste für kritische Infrastrukturen bilden.

(131) Als Reaktion auf die Herausforderungen für die Sicherheit der IKT-Lieferketten, die sich aus nicht technischen Risiken ergeben, haben einige Mitgliedstaaten Regulierungsmaßnahmen ergriffen, wie die Benennung von Hochrisikoanbietern,

---

64 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: https://eur-lex.europa.eu/eli/dir/2022/2555/oj).

65 Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

66 Gemeinsame Mitteilung an das Europäische Parlament und den Rat über die Stärkung der wirtschaftlichen Sicherheit der EU, 3. Dezember 2025 (JOIN(2025) 977 final).

während andere Mitgliedstaaten diesem Beispiel wahrscheinlich folgen werden. Dies könnte zu weiteren Divergenzen zwischen den nationalen Ansätzen und letztlich zu einer höheren Anfälligkeit einiger Mitgliedstaaten führen, mit potenziellen Spillover-Effekten in der gesamten Union. Daher ist es erforderlich, bestimmte Aspekte im Zusammenhang mit den nicht technischen Cybersicherheitsrisiken in den IKT-Lieferketten zu harmonisieren. Ein solches Tätigwerden auf Unionsebene ist auch dadurch gerechtfertigt, dass ein hohes Maß an Cybersicherheit in der gesamten Union gewährleistet werden muss. Die Bestimmungen über die Sicherheit der IKT-Lieferketten zielen darauf ab, solche großen Divergenzen zwischen den Mitgliedstaaten zu beseitigen, insbesondere durch die Festlegung von Vorschriften für Mechanismen zur Risikobewertung von Sicherheitsrisiken in den IKT-Lieferketten auf Unionsebene und von Mindeststandards für den Schutz vor Risiken in IKT-Lieferketten.

(132) Um kritische Abhängigkeiten und Schwachstellen zu verringern, muss ein Rahmen für vertrauenswürdige IKT-Lieferketten geschaffen werden, mit dem nicht technische Risiken im Zusammenhang mit Hochrisikoanbietern und Abhängigkeiten in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren bewältigt werden sollten. Daher ist es notwendig, einen objektiven, risikobasierten, zukunftssicheren und technologieneutralen Rahmen auf Unionsebene zu schaffen, um wichtige IKT-Assets zu ermitteln und eine Reihe verhältnismäßiger Risikominderungsmaßnahmen zur Bewältigung der Risiken vorzusehen.

(133) Cybersicherheitsrisiken, einschließlich Risiken aufgrund der Abhängigkeit von Hochrisikoanbietern, lassen sich in mehreren kritischen IKT-Lieferketten in der Union beobachten, u. a. bei Detektionsgeräten, vernetzten und automatisierten Fahrzeugen, Stromversorgungssystemen, der Stromspeicherung, Wasserversorgungssystemen, Drohnen und Drohnenabwehrsystemen, Cloud-Computing-Diensten, medizinischen Geräten, Überwachungsausrüstung, Weltraumdiensten und Halbleitern. So könnten böswillige Akteure beispielsweise über Schwachstellen bei Sicherheitskontrollgeräten Zugang zu IKT-Systemen erlangen und dadurch Scanner so manipulieren, dass verbotene Gegenstände durch die Sicherheitskontrolle geschleust werden könnten, ohne aufzufallen – mit möglicherweise katastrophalen Folgen.

(134) Diese Verordnung sollte die Mitgliedstaaten nicht daran hindern, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau im Bereich der Sicherheit der IKT-Lieferketten gewährleisten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen. Durch solche Bestimmungen können beispielsweise strengere Risikominderungsmaßnahmen für die wichtigsten IKT-Assets vorgeschrieben werden.

(135) Um potenzielle Cybersicherheitsrisiken für bestimmte IKT-Lieferketten zu ermitteln, kann die mit Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzte Kooperationsgruppe (im Folgenden „NIS-Kooperationsgruppe“) bestimmte IKT-Lieferketten im Rahmen von auf Unionsebene koordinierten Sicherheitsrisikobewertungen bewerten. Bei den auf Unionsebene koordinierten Sicherheitsrisikobewertungen sollten unter anderem die wichtigsten Bedrohungsakteure sowie die größten Bedrohungen und Schwachstellen, die sich auf die wichtigsten IKT-Assets auswirken, untersucht werden. Im Rahmen der auf Unionsebene koordinierten Sicherheitsrisikobewertungen sollte eine Liste von Risikoszenarien und eine Liste von Maßnahmen zur Minderung der Risiken erstellt werden. Auf Unionsebene koordinierte Sicherheitsrisikobewertungen sollten innerhalb

von sechs Monaten abgeschlossen sein. In besonders dringenden Fällen sollte es möglich sein, die Fristen zu verkürzen.

(136) Hat die Kommission hinreichenden Grund zu der Annahme, dass eine erhebliche Cyberbedrohung für die Sicherheit der Union im Zusammenhang mit kritischen IKT-Lieferketten besteht und eine Maßnahme erforderlich sein könnte, um das reibungslose Funktionieren des Binnenmarkts zu erhalten, sollte sie unverzüglich die Mitgliedstaaten zur Notwendigkeit von Risikominderungsmaßnahmen konsultieren und unter Berücksichtigung der Konsultation der Mitgliedstaaten eine Sicherheitsrisikobewertung vornehmen.

(137) Ergibt eine von der NIS-Kooperationsgruppe oder der Kommission vorgenommene Sicherheitsrisikobewertung, dass von einem bestimmten Drittland schwerwiegende, strukturelle nicht technische Cybersicherheitsrisiken für die IKT-Lieferketten ausgehen, so sollte die Kommission die von diesem Land ausgehende Bedrohung überprüfen. Die Kommission kann eine solche Überprüfung auch auf der Grundlage anderer Quellen einleiten, z. B. einer öffentlichen Erklärung im Namen der Union oder eines Mitgliedstaats als Reaktion auf unverantwortliches staatliches Handeln im Cyberraum, das zu einem Cybersicherheitsvorfall geführt hat. Um das Ausmaß der Bedrohung zu bewerten, sollte die Kommission Elemente wie das Bestehen von Rechtsvorschriften oder Praktiken in dem betreffenden Drittland berücksichtigen, nach denen die seiner rechtlichen Zuständigkeit unterliegenden Einrichtungen verpflichtet sind, den Behörden dieses Drittlands Informationen über Schwachstellen bei Software oder Hardware zu melden, bevor bekannt wird, dass diese Schwachstellen ausgenutzt wurden. Ein weiteres wichtiges Element ist das Fehlen wirksamer Rechtsbehelfe und unabhängiger, demokratischer Kontrollmechanismen, mit denen Sicherheitsbedenken ausgeräumt werden können, auch in Bezug auf bestehende Praktiken, fundierte Informationen über Sicherheitsvorfälle, die von Bedrohungsakteuren ausgehen, welche von diesem Land aus kontrolliert werden, vom Hoheitsgebiet dieses Landes aus tätig sind und böswillige Cyberaktivitäten oder -kampagnen durchführen, und die mangelnde Fähigkeit oder Bereitschaft des Drittlands, mit der Kommission oder den Mitgliedstaaten zusammenzuarbeiten, um dem Risiko zu begegnen, das sich aus dem Handeln solcher Bedrohungsakteure ergibt. Die Kommission sollte auch Informationen aus auf Unionsebene koordinierten Sicherheitsrisikobewertungen oder aus Berichten von Mitgliedstaaten oder internationalen Organisationen wie der NATO berücksichtigen.

(138) Für die Zwecke dieser Verordnung sollte der Begriff „Kontrolle“ als die Fähigkeit verstanden werden, unmittelbar oder mittelbar durch einen oder mehrere zwischengeschaltete Rechtsträger einen bestimmenden Einfluss auf einen Rechtsträger auszuüben. Eine Kontrolle durch eine Einrichtung aus einem Drittland, für das Cybersicherheitsbedenken bestehen, sollte auch vorliegen, wenn diese Einrichtung über Leitungs- und Verwaltungsstrukturen in diesem Land verfügt.

(139) Die Union sollte keine Projekte finanzieren, an denen Hochrisikoanbieter beteiligt sind, da dies die Sicherheit der Union gefährden und die Interessen und die Glaubwürdigkeit der Union untergraben würde. Hochrisikoanbieter nach dieser Verordnung sollten daher nicht berechtigt sein, im Zusammenhang mit der Bereitstellung von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die in bestimmten wichtigen IKT-Assets verwendet werden sollen, an Finanzierungsprogrammen und -instrumenten der Union, die in direkter und indirekter Mittelverwaltung gemäß Artikel 136 der Verordnung (EU/Euratom) 2024/2509 und gemäß sektorspezifischen Vorschriften der Union

durchgeführt werden, sowie an Finanzierungstätigkeiten der Union, die in geteilter Mittelverwaltung durchgeführt werden, teilzunehmen, auch nicht im nächsten mehrjährigen Finanzrahmen. Durchführungspartner der Union wie die Europäische Investitionsbank-Gruppe und nationale Förderbanken und -institute sollten davon absehen, Projekte zu unterstützen, die im Widerspruch zu den vorstehenden Ausführungen stehen, auch bei Vorhaben auf eigenes Risiko.

(140) Die Vergabe öffentlicher Aufträge kann ein starkes Instrument für Behörden sein, um zu einer innovativeren, nachhaltigeren und wettbewerbsfähigeren Wirtschaft beizutragen und öffentliche Gelder strategisch einzusetzen. Die Vergabe öffentlicher Aufträge im Zusammenhang mit IKT-Lieferketten sollte nicht dazu genutzt werden, Anbieter zu begünstigen, die die Sicherheit der kritischen Infrastruktur der Union bedrohen. Hochrisikoanbieter nach dieser Verordnung sollten daher nicht berechtigt sein, an öffentlichen Vergabeverfahren für die Bereitstellung von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die in bestimmten wichtigen IKT-Assets verwendet werden sollen, teilzunehmen.

(141) Die Cybersicherheitszertifizierung dient der Stärkung der allgemeinen Sicherheit und der Abwehr von Cyberbedrohungen und ist dabei ein Vertrauensmaßstab. Dieses Vertrauen könnte untergraben werden, wenn Hochrisikoanbieter Bescheinigungen über Cybersicherheitskompetenzen ausstellen würden, weshalb sie nicht berechtigt sein sollten, die Zulassung als befugter Unionsanbieter von Bescheinigungen individueller Cybersicherheitskompetenzen zu beantragen. Ebenso ist es angezeigt, Hochrisikoanbieter von der Möglichkeit auszuschließen, eine Cybersicherheitszertifizierung im Rahmen des ECCF zu erhalten und akkreditierte Konformitätsbewertungsstellen für die Ausstellung solcher Zertifikate zu werden.

(142) Cybersicherheitsnormen spielen eine entscheidende Rolle für die Sicherheit und Vertrauenswürdigkeit digitaler Infrastrukturen. Es müssen geeignete Maßnahmen ergriffen werden, um für die Normung im Bereich der Cybersicherheit zu sorgen. Die Einbeziehung von Einrichtungen, die in Ländern niedergelassen sind oder von Ländern kontrolliert werden, für die gemäß dieser Verordnung Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen, kann dazu führen, dass Cybersicherheitsnormen in einer Weise beeinflusst werden, die ihre Sicherheit und Vertrauenswürdigkeit untergräbt.

(143) Auf der Grundlage der Ergebnisse der Sicherheitsrisikobewertungen kann die Kommission im Wege von Durchführungsrechtsakten festlegen, welche IKT-Assets aufgrund ihrer Kritikalität als wichtige IKT-Assets gelten und spezifischen Risikominderungsmaßnahmen unterliegen sollten. Allein schon die Möglichkeit der Konnektivität der einzelnen Assets sollte ausreichen, um das von ihnen ausgehende Cybersicherheitsrisiko zu berücksichtigen.

(144) Wenn dies zur Erreichung eines hohen Maßes an Cybersicherheit, Cyberresilienz und Vertrauen in der Union erforderlich ist, können die Risikominderungsmaßnahmen auf Einrichtungen in Bezug auf ihre IKT-Lieferketten und insbesondere auf die ermittelten wichtigsten IKT-Assets angewandt werden. Die vorgeschlagenen Risikominderungsmaßnahmen sollten auf der Bewertung potenzieller Risiken und Abhängigkeiten beruhen, einschließlich der potenziellen wirtschaftlichen und gesellschaftlichen Auswirkungen solcher Maßnahmen auf die betreffenden Einrichtungen, die in hochkritischen oder anderen kritischen Sektoren tätig sind, insbesondere auf KMU. Bei der Bewertung der wirtschaftlichen Auswirkungen sollten die Kosten für die Umsetzung der Risikominderungsmaßnahmen berücksichtigt

werden, darunter auch die Länge des Lebenszyklus der relevanten Komponenten der wichtigen IKT-Assets, wenn die Maßnahmen einen Anbieterwechsel umfassen. Zudem sollte bewertet werden, inwieweit alternative Anbieter auf dem Markt verfügbar sind, um die kontinuierliche Erbringung der Dienste sicherzustellen.

(145) Da Risikominderungsmaßnahmen restriktive Auswirkungen auf den internationalen Handel mit Waren und Dienstleistungen haben könnten, sollten sie verhältnismäßig und auf das legitime Ziel ausgerichtet sein, die Cybersicherheit von IKT-Lieferketten im Zusammenhang mit Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art im Einklang mit den internationalen Verpflichtungen der Union sicherzustellen.

(146) Die Verwendung, die Installation oder jede andere Art der Integration von Komponenten, die von Hochrisikoanbietern bereitgestellt werden, beim Betrieb wichtiger IKT-Assets birgt möglicherweise Risiken hinsichtlich späterer Datenübermittlungen in ein Drittland. Risiken können insbesondere dadurch entstehen, dass in dem Drittland kein ausreichendes Schutzniveau für die Daten besteht, z. B. Schutz von Grundrechten, des geistigen Eigentums oder von Geschäftsgeheimnissen oder Schutz vor unrechtmäßigem Zugang zu diesen Daten und deren unrechtmäßiger Nutzung für mögliche künftige Unterbrechungen von Lieferketten und zu Spionagezwecken. Um solche Risiken zu mindern, können Beschränkungen bei der Übermittlung bestimmter Arten von Daten an Drittländer auferlegt werden.

(147) Erhebliche Schwachstellen ergeben sich daraus, dass Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art nicht ausreichend diversifizierte Ausrüstungen verwenden. Wenn man sich auf einen einzigen Anbieter verlässt, führt das zu einer Abhängigkeit von bestimmten Ausrüstungen oder Lösungen. Mangelnde Vielfalt bei den Anbietern erhöht die generelle Anfälligkeit kritischer Infrastrukturen, insbesondere wenn Einrichtungen ihre in sensiblen IKT-Assets verwendeten IKT-Komponenten von einem Anbieter beziehen, der ein hohes Risiko birgt. Die Abhängigkeit wirkt sich auch erheblich auf die nationale und unionsweite Resilienz aus und führt zu punktuellen Ausfällen. Um solche Risiken zu mindern, können Vorgaben gemacht werden, wonach es für bestimmte wichtige IKT-Assets mehr als einen Anbieter geben muss.

(148) Es kann auch sein, dass Einrichtungen der Union wichtige Assets im Sinne dieser Verordnung nutzen. Daher sollten die in dieser Verordnung festgelegten Vorschriften über die Sicherheit von IKT-Lieferketten auch für sie gelten. Um sicherzustellen, dass den Besonderheiten der Einrichtungen der Union Rechnung getragen wird, ist es wichtig, nicht technische Risiken, die im Zusammenhang mit IKT-Lieferketten in Bezug auf Einrichtungen der Union bestehen, bei der Durchführung von auf Unionsebene koordinierten Sicherheitsrisikobewertungen zu berücksichtigen.

(149) Unter außergewöhnlichen Umständen, die ein sofortiges Eingreifen rechtfertigen, um das reibungslose Funktionieren des Binnenmarkts zu erhalten, und wenn es eindeutige Anhaltspunkte dafür gibt, die der Kommission hinreichenden Grund zu der Annahme geben, dass die Verwendung von von einem bestimmten Anbieter bereitgestellten IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, eine erhebliche Cybersicherheitsbedrohung für die wirtschaftlichen oder gesellschaftlichen Tätigkeiten von mindestens drei Mitgliedstaaten darstellt, kann die Kommission in enger Abstimmung mit den Mitgliedstaaten vorschlagen, die Verwendung, Installation oder Integration solcher Komponenten dieses Anbieters

durch Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art zu untersagen.

(150) Um die Verhältnismäßigkeit der ergriffenen Maßnahmen zu gewährleisten, können Einrichtungen, die in einem Drittland niedergelassen sind, für das Cybersicherheitsbedenken bestehen und das gemäß dieser Verordnung benannt wurde, oder die von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert werden, beantragen, von dem Verbot ausgenommen zu werden, Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art mit IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten für deren Verwendung, Installation oder Integration in wichtige IKT-Assets dieser Einrichtung enthalten, zu beliefern und an Verfahren zur Vergabe öffentlicher Aufträge teilzunehmen, die im Einklang mit den Rechtsvorschriften zur Umsetzung der Richtlinien 2014/24/EU[67] und 2014/25/EU des Europäischen Parlaments und des Rates[68] in Bezug auf die Bereitstellung von IKT-Komponenten oder Komponenten, die IKT-Komponenten zur Verwendung in bestimmten wichtigen IKT-Assets enthalten, durchgeführt werden. Zu diesem Zweck sollte die Einrichtung einen eindeutigen Nachweis vorlegen, dass sie wirksame Maßnahmen anwendet, um die nicht technischen Risiken zu bewältigen und sicherzustellen, dass es zu keiner unzulässigen Einflussnahme durch ein Drittland kommt, für das Cybersicherheitsbedenken bestehen.

(151) Elektronische Kommunikationsnetze bilden das Rückgrat eines breiten Spektrums von Diensten, die für das Funktionieren des Binnenmarkts, die Aufrechterhaltung und Ausführung wichtiger gesellschaftlicher und wirtschaftlicher Funktionen – wie Energie, Verkehr, Bank- und Gesundheitswesen, Verteidigung – sowie industrieller Steuerungssysteme unverzichtbar sind. Daher sind diese hochkritischen Netze attraktive Ziele für alle Arten von Cyberangriffen und hybriden Bedrohungen, für Störungen, Spionage, Informationsgewinnung sowie für Betrug und Finanzkriminalität. Die Risikobewertung der NIS-Kooperationsgruppe hinsichtlich der Cybersicherheit und der Resilienz der europäischen Kommunikationsinfrastrukturen und -netze zeigte eine Reihe von Risiken und Bedrohungen, die aus Sicht der Union von strategischer Bedeutung sind, wie z. B. Wiper- bzw. Ransomware-Angriffe, Angriffe auf Lieferketten, unbefugtes Eindringen in Netze und verteilte Überlastungsangriffe (DDoS-Angriffe).

(152) Angesichts der Vernetzung und der gegenseitigen Abhängigkeiten der einzelnen nationalen elektronischen Kommunikationsnetze müssen alle Mitgliedstaaten geeignete Maßnahmen ergreifen, um die Sicherheit ihrer Netze zu gewährleisten. Aus denselben Gründen bedarf es eines wirksamen Rechtsrahmens auf Unionsebene, der auch nicht technische Risiken abdeckt und die Sicherheit miteinander verbundener elektronischer Kommunikationsnetze umfassend gewährleistet.

---

67 Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65, ELI: http://data.europa.eu/eli/dir/2014/24/oj).

68 Richtlinie 2014/25/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die Vergabe von Aufträgen durch Auftraggeber im Bereich der Wasser-, Energie- und Verkehrsversorgung sowie der Postdienste und zur Aufhebung der Richtlinie 2004/17/EG (ABl. L 94 vom 28.3.2014, S. 243, ELI: http://data.europa.eu/eli/dir/2014/25/oj).

(153) Insbesondere die Cybersicherheit von 5G-Netzen ist für die Union von strategischer Bedeutung, da diese Netze das Rückgrat eines breiten Spektrums an Diensten bilden, die für das Funktionieren des Binnenmarkts von wesentlicher Bedeutung sind, und auch für den Aufbau unserer Verteidigungsbereitschaft, auch was die militärische Mobilität betrifft, entscheidend sind. 5G-Netze können eine zuverlässige ultraschnelle Konnektivität bieten, z. B. für die Daten- und Informationsweitergabe, die Drohnenerkennung und die Echtzeitkoordinierung auf dem Gefechtsfeld.

(154) Die 5G-Einführung erfolgt in erster Linie in nicht eigenständigen Netzen, in denen nur das Funkzugangsnetz auf 5G-Technologie aufgerüstet wird, während das übrige Netz nach wie vor auf einem bestehenden 4G-Kernnetz beruht. Nicht eigenständige 5G-Netze bauen in erster Linie auf bereits vorhandener Infrastruktur auf, sodass die Sicherheit künftiger 5G-Netze bis zu einem gewissen Grad von bereits vorhandener Netzausrüstung und der Konfiguration dieser Ausrüstung abhängt. Daher sollten die Risikominderungsmaßnahmen auch für 4G-Netze gelten, die die Grundlage für die 5G-Einführung bilden.

(155) Um wichtigen Sicherheitsherausforderungen in 5G-Netzen zu begegnen, haben die Mitgliedstaaten im Rahmen der NIS-Kooperationsgruppe gemeinsam mit der Kommission und der ENISA eine auf Unionsebene koordinierte Sicherheitsrisikobewertung von 5G-Netzen vorgenommen, bei der sowohl technische als auch nicht technische Risiken untersucht wurden. Bei dieser Bewertung wurden mehrere Risiken ermittelt, darunter die Möglichkeit, dass Drittländer oder Akteure aus Drittländern über die Lieferkette Einfluss nehmen, und die Assets nach ihrer Kritikalität kategorisiert. Diese Bewertung sollte als Grundlage für die Festlegung der wichtigen IKT-Assets für 5G-Kommunikationsnetze dienen.

(156) Zur Minderung der Risiken, die in der koordinierten Sicherheitsrisikobewertung von 5G-Netzen ermittelt wurden, hat die NIS-Kooperationsgruppe das EU-Instrumentarium für die 5G-Cybersicherheit angenommen, das strategische und technische Maßnahmen umfasst. Die meisten Mitgliedstaaten verfügen zwar über Rechtsrahmen, die Beschränkungen für Hochrisikoanbieter oder deren Ausschluss ermöglichen, wie im 5G-Instrumentarium empfohlen, doch diese Rahmen wurden nicht einheitlich umgesetzt. Dies führt dazu, dass viele 5G-Standorte in der gesamten Union von Hochrisikoanbietern beliefert werden, wie in der Mitteilung der Kommission über die Umsetzung des 5G-Instrumentariums[69] dargelegt. Daraus ergeben sich Schwachstellen, einschließlich strategischer Abhängigkeiten und potenzieller Einflussnahme durch Drittländer, was sich auch auf künftige auf bestehenden 5G-Netzen aufbauende 6G-Infrastruktur auswirken könnte. Aufgrund der uneinheitlichen Umsetzung der im Rahmen des 5G-Instrumentariums empfohlenen Maßnahmen, insbesondere was den Umfang der Beschränkungen für Hochrisikoanbieter betrifft, bestehen Unterschiede zwischen den Mitgliedstaaten, die zu ungleichen Wettbewerbsbedingungen führen, was wiederum den Binnenmarkt spaltet und die Netzsicherheit insgesamt schwächt. Der Europäische Rechnungshof hat diese Divergenzen hervorgehoben und davor gewarnt, dass das Fehlen eines koordinierten Ansatzes das Funktionieren des Binnenmarkts untergräbt. Eine anhaltende Abhängigkeit von Hochrisikoanbietern birgt ernsthafte Risiken für die Sicherheit kritischer Infrastrukturen in der Union und könnte das Vertrauen in den Binnenmarkt untergraben, da uneinheitliche Sicherheitsniveaus Verbraucher und

[69] Mitteilung der Kommission über die Umsetzung des Instrumentariums für die 5G-Cybersicherheit, 15. Juni 2023, C(2023) 4049 final.

Unternehmen unionsweit davon abhalten können, 5G-gestützte Produkte und Dienste zu nutzen. Daher ist es von entscheidender Bedeutung, dass auf Unionsebene Maßnahmen ergriffen werden, um einen harmonisierten Ansatz bei der Sicherheit von 5G-Netzen zu gewährleisten.

(157) Zur Festlegung einer Frist für die schrittweise Entfernung der wichtigen IKT-Assets von festen und satellitengestützten elektronischen Kommunikationsnetzen sollte die Kommission eine Bewertung vornehmen, bei der das Ausmaß der Sicherheitsrisiken im Zusammenhang mit den einzelnen wichtigen IKT-Assets der festen und satellitengestützten Netze, die Lebensdauer der relevanten Komponenten und die wirtschaftlichen Auswirkungen, die die Entfernung dieser Komponenten auf die betreffenden Betreiber hätte, gebührend berücksichtigt werden. Auf der Grundlage der Ergebnisse dieser Bewertung kann die Kommission erwägen, unterschiedliche Fristen für die Entfernung bestimmter wichtiger IKT-Assets und deren integraler Bestandteile festzulegen.

(158) Um eine wirksame Aufsicht und Durchsetzung der Verpflichtungen in Bezug auf die Anbieter mobiler, fester und satellitengestützter elektronischer Kommunikationsnetze zu gewährleisten, sollten die nach dieser Verordnung jeweils zuständigen Behörden eng mit den nach dem [DNA-Vorschlag] zuständigen Behörden zusammenarbeiten. Auf Ersuchen einer gemäß dieser Verordnung benannten zuständigen Behörde sollten die nationalen Regulierungsbehörden oder andere für das Frequenzspektrum zuständige Behörden gegebenenfalls die in Artikel 9 und Artikel 20 [DNA-Vorschlag] genannten Rechte entziehen, wenn der Anbieter öffentlicher elektronischer Kommunikationsnetze den Verpflichtungen aus der vorliegenden Verordnung nicht nachkommt, u. a. wenn der Anbieter von Hochrisikoanbietern bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die in wichtigen IKT-Assets verwendet werden sollen, nicht innerhalb der gemäß dieser Verordnung festgelegten Frist schrittweise entfernt.

(159) Angesichts der Unterschiede in den nationalen Governance-Strukturen sollten die Mitgliedstaaten eine oder mehrere zuständige Behörden benennen oder einrichten, die für die Aufsichts- und Durchsetzungsmaßnahmen nach dieser Verordnung zuständig sind.

(160) Die zuständigen Behörden sollten Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art bei der Erfüllung ihrer Verpflichtungen aus dieser Verordnung unterstützen. Zu diesem Zweck sollte die Kommission bewerten, ob Anbieter, die von spezifischen Verboten betroffen sein könnten, in einem Drittland niedergelassen sind, für das Cybersicherheitsbedenken bestehen, oder von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert werden. Die zuständigen Behörden sollten eng mit der Kommission und anderen zuständigen Behörden innerhalb des gemäß dieser Verordnung eingerichteten Netzes zusammenarbeiten. Auf der Grundlage der Bewertung durch die Kommission sollten die zuständigen Behörden einschlägige Informationen über Hochrisikoanbieter an die betreffenden Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art weitergeben. Von den Einrichtungen wird nicht erwartet, dass sie überprüfen, ob ein Anbieter unter ausländischer Kontrolle steht; sie können sich vollumfänglich auf die von den zuständigen Behörden erhaltenen Informationen verlassen. Die zuständigen Behörden sollten sicherstellen, dass diesen Einrichtungen kein unnötiger Verwaltungsaufwand aufgebürdet wird.

(161) Um die wirksame Einhaltung der Vorschriften zu gewährleisten, sollte diese Verordnung Aufsichts- und Durchsetzungsmaßnahmen enthalten, mit denen die zuständigen Behörden Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art beaufsichtigen können. Bei der Wahrnehmung ihrer Aufsichts- und Durchsetzungsaufgaben gegenüber diesen Einrichtungen sollten die zuständigen Behörden nicht über das erforderliche Maß hinausgehen und ein angemessenes Verhältnis zu den ermittelten Risiken wahren.

(162) Um eine wirksame und einheitliche Durchsetzung in der gesamten Union zu gewährleisten, müssen die zuständigen Behörden Durchsetzungsbefugnisse erhalten, die sie bei Verstößen gegen die in dieser Verordnung festgelegten Verpflichtungen ausüben können. Bei der Ausübung dieser Durchsetzungsbefugnisse sollten die zuständigen Behörden einer Reihe von Faktoren gebührend Rechnung tragen; hierzu zählen die Art, Schwere und Dauer des Verstoßes, der entstandene materielle oder immaterielle Schaden, die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, die Maßnahmen zur Vermeidung oder Minderung des entstandenen materiellen oder immateriellen Schadens, der Grad der Verantwortlichkeit oder jeglicher früherer Verstoß, der Umfang der Zusammenarbeit mit der zuständigen Behörde sowie jeder andere erschwerende oder mildernde Umstand. Die Durchsetzungsmaßnahmen, einschließlich Sanktionen, sollten verhältnismäßig sein, und für die Verhängung sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht sowie der Unschuldsvermutung und der Verteidigungsrechte, entsprechen.

(163) Wichtig ist auch, die Befugnis vorzusehen, Zwangsgelder zu verhängen, um eine Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art zu zwingen, einen Verstoß gegen diese Verordnung gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen.

(164) Um die wirksame Durchsetzung der in dieser Verordnung festgelegten Verpflichtungen zu gewährleisten, sollte jede zuständige Behörde befugt sein, Sanktionen zu verhängen oder deren Verhängung zu beantragen.

(165) Wenn Sanktionen gegen eine Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art verhängt werden, bei der es sich um ein Unternehmen handelt, sollte ein Unternehmen als Unternehmen im Sinne der Artikel 101 und 102 AEUV verstanden werden. Wird einer Person, bei der es sich nicht um ein Unternehmen handelt, eine Geldbuße auferlegt, so sollte die zuständige Behörde bei der geeigneten Bemessung der Sanktion dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Sanktionen verhängt werden können. Die Verhängung einer Sanktion sollte die Ausübung anderer Befugnisse der zuständigen Behörden nicht beeinträchtigen.

(166) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden in Bezug auf den Erlass von Durchführungsrechtsakten zur Festlegung von Durchführungsbestimmungen über die von der ENISA erhobenen Gebühren, von Durchführungsrechtsakten zur Einrichtung eines europäischen Systems für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen, von Durchführungsrechtsakten zur Festlegung gemeinsamer Grundsätze sowie von

Referenzbestimmungen zur Festlegung von Elementen in allen europäischen Systemen für die Cybersicherheitszertifizierung, von Durchführungsrechtsakten zur Festlegung der Verfahren für Modelle der vorherigen Zustimmung oder der allgemeinen Übertragung, von Durchführungsrechtsakten zur Anerkennung der Gleichwertigkeit von Cybersicherheitszertifikaten eines Drittlands oder einer internationalen Organisation mit europäischen Cybersicherheitszertifikaten, von Durchführungsrechtsakten zur Festlegung eines Plans für die gegenseitige Begutachtung, von Durchführungsrechtsakten zur Festlegung der Verfahren, auch bei der grenzüberschreitenden Zusammenarbeit, für die Zulassung von Konformitätsbewertungsstellen, von Durchführungsrechtsakten zur Festlegung der Umstände, Formate und Verfahren für Notifizierungen von Konformitätsbewertungsstellen, von Durchführungsrechtsakten zur Benennung eines Drittlands als Land, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen, von Durchführungsrechtsakten zur Ermittlung der wichtigen IKT-Assets, die für die Herstellung von Produkten oder die Erbringung von Dienstleistungen durch Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art verwendet werden, von Durchführungsrechtsakten zur Festlegung, dass in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren tätige Einrichtungen spezifischen Risikominderungsmaßnahmen unterliegen, und zur Festlegung der Fristen für die schrittweise Entfernung der von Hochrisikoanbietern bereitgestellten IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, von Durchführungsrechtsakten zur präziseren Festlegung der Bedingungen für die Ausnahmen für Einrichtungen, die in einem Drittland, für das Bedenken in Bezug auf die Cybersicherheit bestehen, niedergelassen sind oder von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert werden, sowie von Durchführungsrechtsakten zur Festlegung von Durchführungsbestimmungen über die von der Kommission erhobenen Gebühren. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden, und das Prüfverfahren sollte zur Anwendung kommen. Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission auch Durchführungsbefugnisse zur Erstellung einer für bestimmte Maßnahmen gemäß dieser Verordnung relevanten Liste von Hochrisikoanbietern übertragen werden.

(167) Es ist notwendig, dass die europäischen Systeme für die Cybersicherheitszertifizierung den neuesten technologischen Entwicklungen, neuen damit verbundenen Bedrohungen und der Annahme neuer Rechtsvorschriften der Union Rechnung tragen, in denen der Nachweis der Konformität und die Vermutung der Konformität mit den einschlägigen Cybersicherheitsanforderungen dieser Rechtsvorschriften durch die europäische Cybersicherheitszertifizierung geregelt sind. Aus diesen Gründen sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zu erlassen, um Sicherheitsziele, die mit den europäischen Systemen für die Cybersicherheitszertifizierung verfolgt werden, hinzuzufügen oder zu ändern. Ebenso sollte der Kommission im Interesse eines Rahmens für vertrauenswürdige IKT-Lieferketten die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Änderung des Anhangs II dieser Verordnung zu erlassen, um ihn an technologische Entwicklungen anzupassen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung festgelegt wurden. Um insbesondere für eine gleichberechtigte

Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, sollten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten erhalten, und ihre Sachverständigen sollten systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission haben, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(168) Die Tätigkeit der ENISA sollte regelmäßig und unabhängig bewertet werden. Diese Bewertung sollte sich auf die Ziele der ENISA und die Relevanz ihrer Aufgaben beziehen, insbesondere ihre Aufgaben bezüglich der operativen Zusammenarbeit auf Unionsebene. Im Falle einer Überprüfung sollte die Kommission bewerten, inwieweit die Rolle der ENISA als Bezugspunkt für Beratung und Sachkenntnis gestärkt werden kann.

(169) Die Durchführungsverordnung (EU) 2024/482 der Kommission enthält Vorschriften für die Annahme des auf den Gemeinsamen Kriterien beruhenden europäischen Systems für die Cybersicherheitszertifizierung (EUCC). Das EUCC ist das erste und einzige europäische System für die Cybersicherheitszertifizierung, das gemäß der Verordnung (EU) 2019/881 angenommen wurde. Es betrifft die Zertifizierung von IKT-Produkten, einschließlich Produkten der technischen Bereiche „Chipkarten und ähnliche Geräte“ und „Hardware-Geräte mit Sicherheitsboxen“, sowie Schutzprofilen (als IKT-Prozesse). Daher muss sichergestellt werden, dass die Notifizierungstätigkeiten sowie die Arbeit der Agentur fortgesetzt werden.

(170) Der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss wurden gemäß Artikel 42 Absatz 2 der Verordnung (EU) 2018/1725[70] angehört und haben am [Datum] eine gemeinsame Stellungnahme abgegeben.

(171) Die Verordnung (EU) 2019/881 sollte aufgehoben werden.

(172) Da die Ziele dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs und ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand und Anwendungsbereich

(1) Mit dieser Verordnung wird Folgendes festgelegt:

a) Auftrag, Ziele, Aufgaben und organisatorische Aspekte der Agentur der Europäischen Union für Cybersicherheit (ENISA),

---

[70] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

b) ein Rahmen für die Festlegung europäischer Systeme für die Cybersicherheitszertifizierung, mit dem Ziel, für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten, und mit dem Ziel, eine Fragmentierung des Binnenmarkts für Systeme für die Cybersicherheitszertifizierung in der Union zu verhindern, und

c) ein Rahmen für vertrauenswürdige IKT-Lieferketten.

(2) Der in Absatz 1 Buchstabe b genannte Rahmen gilt unbeschadet besonderer Bestimmungen in anderen Rechtsakten der Union für eine freiwillige oder eine verbindliche Zertifizierung.

(3) Der in Absatz 1 Buchstabe c genannte Rahmen gilt für öffentliche oder private Einrichtungen einer in Anhang I oder II der Richtlinie (EU) 2022/2555 genannten Art, die ihre Dienste in der Union anbieten oder ihre Tätigkeiten dort ausüben.

(4) Diese Verordnung lässt die grundlegenden staatlichen Funktionen der Mitgliedstaaten, darunter auch die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit, unberührt. Insbesondere die nationale Sicherheit fällt weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Cybersicherheit“ alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

2. „Einrichtungen der Union“ Einrichtungen der Union im Sinne des Artikels 3 Nummer 1 der Verordnung (EU, Euratom) 2023/2841;

3. „befugter Bescheinigungsanbieter“ eine öffentliche oder private Einrichtung, der die ENISA mit einem Beschluss die Befugnis übertragen hat, europäische Einzelbescheinigungen von Cybersicherheitskompetenzen nach einem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen auszustellen;

4. „europäische Einzelbescheinigung von Cybersicherheitskompetenzen“ eine digitale oder physische Aufzeichnung, mit der bescheinigt wird, dass eine Einzelperson die mit einem Rollenprofil oder einer Teilmenge eines Rollenprofils des europäischen Rahmens für Cybersicherheitskompetenzen (im Folgenden „ECSF“) verbundenen Aufgaben kennt, versteht und erfüllen kann, und zwar im Anschluss an eine Bewertung nach einem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen;

5. „System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen“ ein umfassendes Paket von Vorschriften, Anforderungen, Normen und Verfahren, die von der ENISA festgelegt wurden und einem ECSF-Rollenprofil oder einer Teilmenge davon zugeordnet sind und die für befugte Bescheinigungsanbieter gelten und von diesen angewandt werden;

6. „Netz- und Informationssystem“ ein Netz- und Informationssystem im Sinne des Artikels 6 Nummer 1 der Richtlinie (EU) 2022/2555;

7. „nationale Cybersicherheitsstrategie“ eine nationale Cybersicherheitsstrategie im Sinne des Artikels 6 Nummer 4 der Richtlinie (EU) 2022/2555;

8. „Sicherheitsvorfall“ einen Sicherheitsvorfall im Sinne des Artikels 6 Nummer 6 der Richtlinie (EU) 2022/2555;

9. „Cybersicherheitsvorfall großen Ausmaßes“ einen Cybersicherheitsvorfall großen Ausmaßes im Sinne des Artikels 6 Nummer 7 der Richtlinie (EU) 2022/2555;

10. „Bewältigung von Sicherheitsvorfällen“ die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 6 Nummer 8 der Richtlinie (EU) 2022/2555;

11. „Cyberbedrohung“ einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;

12. „europäisches System für die Cybersicherheitszertifizierung“ ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen gelten;

13. „nationales System für die Cybersicherheitszertifizierung“ ein umfassendes, von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die für die Zertifizierung oder Konformitätsbewertung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen gelten, die von diesem System erfasst werden;

14. „europäisches Cybersicherheitszertifikat“ ein von einer maßgeblichen Stelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst, ein bestimmter IKT-Prozess, ein bestimmter verwalteter Sicherheitsdienst oder die Cyberabwehr einer Einrichtung im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europäischen System für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde;

15. „EU-Konformitätserklärung“ ein von einem Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder einer Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist, ausgestelltes Dokument, in dem bescheinigt wird, dass die Erfüllung der im europäischen System für die Cybersicherheitszertifizierung festgelegten Anforderungen der Vertrauenswürdigkeitsstufe „niedrig“ durch eine Selbstbewertung der Konformität nachgewiesen wurde;

16. „IKT-Produkt“ ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;

17. „IKT-Dienst“ einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;

18. „IKT-Prozess“ jegliche Tätigkeiten, mit denen ein IKT-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;

19. „verwalteter Sicherheitsdienst“ einen für einen Dritten erbrachten Dienst, der in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement besteht, wie beispielsweise die Bewältigung von Sicherheitsvorfällen, Penetrationstests, Sicherheitsaudits und Beratung – auch durch Sachverständige – zur technischen Unterstützung;

20. „Akkreditierung“ eine Akkreditierung im Sinne des Artikels 2 Nummer 10 der Verordnung (EG) Nr. 765/2008;

21. „nationale Akkreditierungsstelle“ eine nationale Akkreditierungsstelle im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 765/2008;

22. „Konformitätsbewertung“ eine Konformitätsbewertung im Sinne des Artikels 2 Nummer 12 der Verordnung (EG) Nr. 765/2008;

23. „Konformitätsbewertungsstelle“ eine Konformitätsbewertungsstelle im Sinne des Artikels 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

24. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[71];

25. „technische Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012;

26. „harmonisierte Norm“ eine harmonisierte Norm im Sinne des Artikels 2 Nummer 1 Buchstabe c der Verordnung (EU) Nr. 1025/2012;

27. „Vertrauenswürdigkeitsstufe“ die Grundlage für das Vertrauen darin, dass ein IKT-Produkt, -Dienst oder -Prozess, ein verwalteter Sicherheitsdienst oder die Cyberabwehr einer Einrichtung den Sicherheitsanforderungen eines spezifischen europäischen Systems für die Cybersicherheitszertifizierung genügt; sie gibt an, auf welchem Niveau das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, der verwaltete Sicherheitsdienst oder die Cyberabwehr der Einrichtung bei der Bewertung eingestuft wurde, ist jedoch als solche kein Maß für die Sicherheit des jeweiligen IKT-Produkts, -Dienstes, -Prozesses, verwalteten Sicherheitsdienstes oder der Cyberabwehr der betreffenden Einrichtung;

28. „Selbstbewertung der Konformität“ eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder der Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist, zur Bewertung, ob diese IKT-Produkte, -Dienste oder -Prozesse, verwalteten Sicherheitsdienste oder die Cyberabwehr von Einrichtungen die Anforderungen, die in einem bestimmten europäischen System für die Cybersicherheitszertifizierung festgelegt sind, erfüllen;

29. „Cyberabwehr von Einrichtungen“ das Cybersicherheitsniveau von Einrichtungen in Bezug auf die besonderen Sicherheitsanforderungen;

---

[71] Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

30. „Modell der vorherigen Zustimmung“ ein Modell, bei dem eine Konformitätsbewertungsstelle ein europäisches Cybersicherheitszertifikat auf der Grundlage der Bewertung durch eine nationale Behörde für die Cybersicherheitszertifizierung im Rahmen eines bestimmten Zertifizierungsverfahrens nach einem einschlägigen System ausstellen kann;

31. „Modell der allgemeinen Übertragung“ ein Modell, bei dem eine Konformitätsbewertungsstelle ein europäisches Cybersicherheitszertifikat auf der Grundlage einer Übertragung von Zertifizierungstätigkeiten durch eine nationale Behörde für die Cybersicherheitszertifizierung ausstellen kann;

32. „Computer-Notfallteam“ oder „CSIRT“ ein gemäß Artikel 10 der Richtlinie (EU) 2022/2555 benanntes oder eingerichtetes CSIRT;

33. „IKT-Komponenten“ IKT-Produkte, -Dienste oder -Prozesse, die für den Betrieb von IKT-Assets verwendet werden können;

34. „IKT-Assets“ Software oder Hardware in den Netz- und Informationssystemen, die von einer Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art verwendet werden;

35. „wichtige IKT-Assets“ IKT-Assets, die gemäß Artikel 102 ermittelt wurden;

36. „elektronisches Kommunikationsnetz“ ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) XX/XXXX [Vorschlag für die Verordnung über digitale Netze, DNA-Vorschlag];

37. „Kontrolle“ die Fähigkeit, unmittelbar oder mittelbar durch einen oder mehrere zwischengeschaltete Rechtsträger einen bestimmenden Einfluss auf einen Rechtsträger auszuüben;

38. „Niederlassung“ die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung in dem Land, in dem die Einrichtung ihre Hauptverwaltung oder ihren Hauptgeschäftssitz hat;

39. „Hochrisikoanbieter“ einen der folgenden Anbieter:

    a) eine Einrichtung, die in einem Drittland, für das Cybersicherheitsbedenken bestehen und das gemäß Artikel 100 benannt wurde, niedergelassen ist oder die von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert wird;

    b) eine gemäß Artikel 103 Absatz 7 benannte Einrichtung und von ihr kontrollierte Einrichtungen;

40. „IKT-Lieferkette“ eine Gesamtheit von IKT-Diensten, -Produkten und -Prozessen, die Tätigkeiten und Akteure umfasst, die auf allen Stufen vor der Bereitstellung eines Produkts oder eines Dienstes auf dem Markt beteiligt sind;

41. „Drittland“ ein Drittland im Sinne des Artikels 3 Nummer 4 der Verordnung (EU) 2023/2675 des Europäischen Parlaments und des Rates[72];

[72] Verordnung (EU) 2023/2675 des Europäischen Parlaments und des Rates vom 22. November 2023 über den Schutz der Union und ihrer Mitgliedstaaten vor wirtschaftlichem Zwang durch Drittländer (ABl. L, 2023/2675, 7.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2675/oj).

42. „nicht technisches Risiko“ die Wahrscheinlichkeit, dass der Anbieter dem Einfluss eines Drittlands steht und dies zu einem Verlust oder einer Störung des bereitgestellten Dienstes oder zu einer Beeinträchtigung des von einer Einrichtung hergestellten Produkts oder zu einer Datenexfiltration, auch zu Zwecken der Spionage oder der Erzielung von Einnahmen führen könnte;

43. „erhebliches nicht technisches Cybersicherheitsrisiko“ ein nicht technisches Cybersicherheitsrisiko, bei dem davon auszugehen ist, dass es mit hoher Wahrscheinlichkeit zu einem Sicherheitsvorfall führen wird, der schwerwiegende negative Auswirkungen haben und erhebliche materielle oder immaterielle Verluste oder Störungen verursachen könnte;

44. „Kernnetzfunktionen von mobilen elektronischen Kommunikationsnetzen“ das zentrale architektonische Element der elektronischen Mobilfunk-Kommunikationsnetze, mit dem wichtige Netzknoten mit dem Internet verbunden und wesentliche Systemfunktionen verwaltet werden, wozu die Authentifizierung der Nutzergeräte, Funktionen der rechtmäßigen Überwachung (LI), Sicherheitsgateways (SeGW) am Netzrand, Signalisierungssicherheitsfunktionen, die Roaming- und Sitzungsverwaltung, der Datentransport auf Nutzer- und Steuerungsebene, die Verwaltung der Zugangsregelungen, die Registrierung und Genehmigung von Netzdiensten, die Speicherung von Endnutzer- und Netzdaten, kritische Netzdienste einschließlich des Domänennamensystems (DNS), die Zusammenschaltung mit Mobilfunknetzen Dritter, die Exposition von Kernnetzfunktionen gegenüber externen Anwendungen sowie die Auswahl und Verwaltung von virtuellen Teilnetzen (Network Slices) gehören;

45. „Virtualisierung von Netzfunktionen (NFV) sowie Verwaltung und Netzorchestrierung (MANO) von mobilen elektronischen Kommunikationsnetzen“ die Software und den architektonischen Rahmen, die das Lebenszyklusmanagement, die Orchestrierung und die Automatisierung virtueller Netzfunktionen (VNFs), Cloud-nativer Netzfunktionen (CNFs) und die Auswahl und Verwaltung von virtuellen Teilnetzen (Network Slices) in elektronischen Mobilfunk-Kommunikationsnetzen gewährleisten;

46. „Funkzugangsnetz (RAN) von mobilen elektronischen Kommunikationsnetzen“ das Netz, das Mobilfunk-Nutzerausrüstung mit dem Kernnetz verbindet, einschließlich Basisstationen (eNodeB für 4G, gNodeB für 5G), abgesetzter Funkköpfe (RRH) und Basisbandeinheiten (BBU), aktiver Antennensysteme (AAS) und gegebenenfalls disaggregierter RAN-Komponenten wie Zentraleinheiten (CU) und verteilter Einheiten (DU) sowie der intelligenten RAN-Steuerung (RIC);

47. „Kernnetzfunktionen von festen elektronischen Kommunikationsnetzen“ die Backbone-Intelligenz des Netzes, die die wichtigsten Knoten miteinander verbindet und eine Reihe wesentlicher Funktionen regelt, darunter die Nutzerauthentifizierung und -autorisierung (AAA), Funktionen der rechtmäßigen Überwachung (LI), das Domänennamensystem (DNS) und IP-Adressierungsdienste (DHCP), die Verwaltung der Zugangsregelungen, die Speicherung von Endnutzer- und Netzdaten, IP-Switching und -Routing sowie internationale Internet-Gateways (IIG);

48. „Netzmanagementsystem von festen elektronischen Kommunikationsnetzen“ alle zentralen Plattformen und Softwarekomponenten, die für den Betrieb, die Verwaltung, Wartung und Bereitstellung (OAM&P) des Netzes und die Überwachung netzbezogener Informationen erforderlich sind;

49. „Transport- und Übertragungsfunktionen von festen elektronischen Kommunikationsnetzen“ alle Komponenten, die für den Backhaul und die Aggregierung des Verkehrs im gesamten Netz erforderlich sind, einschließlich Ausrüstungen für den optischen Transport, Mikrowellenverbindungen und Seekabelsystemen, wozu auch die Unterwasserausrüstung, landseitige Seekabelendeinrichtungen (SLTE) und die physischen Landungsstellenanlagen gehören;

50. „Zugangsnetz von festen elektronischen Kommunikationsnetzen“ das Netz, das die Räumlichkeiten des Endnutzers mit dem Aggregations- oder Kernnetz verbindet, einschließlich des optischen Leitungsabschlusses (OLT) und des optischen Netzabschlusses (ONT) für Glasfasernetze, des Koaxialkabelmodem-Abschlusssystems (CMTS) und des Kabelmodems für Koaxialkabelnetze sowie Komponenten für den drahtlosen Festnetzzugang, sofern sie als Substitut für Festnetzanschlüsse verwendet werden.

TITEL II
DIE AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT

Kapitel I
Auftrag und Ziele

Artikel 3
Auftrag der ENISA

(1) Die ENISA hat den Auftrag, die Mitgliedstaaten und die Einrichtungen der Union dabei zu unterstützen, in der Union ein hohes Maß an Cybersicherheit, Cyberresilienz und Vertrauen zu erreichen.

(2) Die ENISA dient den Mitgliedstaaten sowie anderen Interessenträgern in der Union als Bezugspunkt für Beratung und Sachkenntnis im Bereich Cybersicherheit.

(3) Die ENISA trägt durch die Wahrnehmung der ihr mit dieser Verordnung zugewiesenen Aufgaben zur Verringerung der Fragmentierung im Binnenmarkt bei.

(4) Die ENISA nimmt die ihr durch Rechtsakte der Union zugewiesenen Aufgaben wahr.

(5) Die ENISA entwickelt ihre eigenen Fähigkeiten, einschließlich technischer und menschlicher Fähigkeiten und Fertigkeiten, die erforderlich sind, um die ihr mit dieser Verordnung zugewiesenen Aufgaben wahrzunehmen.

Artikel 4
Ziele der ENISA

(1) Die ENISA dient aufgrund ihrer Unabhängigkeit, der wissenschaftlichen und technischen Qualität der von ihr geleisteten Beratung, Beiträge und Unterstützung, der von ihr bereitgestellten Informationen, der Transparenz ihrer operativen Verfahren, ihrer Arbeitsmethoden sowie der Sorgfalt bei der Wahrnehmung ihrer Aufgaben als Kompetenzzentrum in Fragen der Cybersicherheit.

(2) Die ENISA unterstützt die Mitgliedstaaten und gegebenenfalls Einrichtungen der Union bei der Umsetzung horizontaler und sektoraler Strategien und

Rechtsvorschriften der Union im Zusammenhang mit der Cybersicherheit, einschließlich Marktüberwachungstätigkeiten.

(3) Die ENISA stellt ihre Sachkenntnis zur Verfügung und unterstützt die Kommission bei der Entwicklung von Strategien und Rechtsvorschriften der Union im Bereich der Cybersicherheit.

(4) Die ENISA fördert unionsweit den Kapazitätsaufbau und die Abwehrbereitschaft, indem sie die Mitgliedstaaten und Einrichtungen der Union mithilfe des in Kapitel IV der Verordnung (EU, Euratom) 2023/2841 genannten Cybersicherheitsdienstes für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) sowie öffentliche und private Interessenträger dabei unterstützt, den Schutz ihrer Netz- und Informationssysteme zu verstärken und Fähigkeiten zur Abwehr von Cyberangriffen und Reaktionskapazitäten aufzubauen und zu verbessern.

(5) Die ENISA trägt zur Einrichtung der Akademie für Cybersicherheitskompetenzen und zum Ausbau der Fachkräftebasis im Bereich Cybersicherheit in der Union bei, indem sie die Bemühungen um die Entwicklung der Übertragbarkeit von Kompetenzen in der gesamten Union unterstützt, unter anderem durch die Pflege und Nutzung des ECSF sowie die Entwicklung, Pflege und Verbreitung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Kapitel II Abschnitt 4 dieses Titels, und indem sie die Durchführung von Fortbildungen gemäß Artikel 6 Absatz 8 sicherstellt.

(6) Die ENISA fördert auf Unionsebene die Zusammenarbeit, einschließlich der Informationsweitergabe und der Koordinierung, zwischen den Mitgliedstaaten und den Einrichtungen der Union im Einklang mit der Verordnung (EU, Euratom) 2023/2841 sowie den einschlägigen privaten und öffentlichen Interessenträgern in Fragen, die im Zusammenhang mit der Cybersicherheit stehen.

(7) Die ENISA trägt zum Ausbau der Cybersicherheitskapazitäten auf Unionsebene bei, um die Maßnahmen zu unterstützen, die die Mitgliedstaaten zur Vermeidung von Cyberbedrohungen oder als Reaktion darauf ergreifen.

(8) Die ENISA unterstützt die operative Zusammenarbeit auf Unionsebene, unter anderem durch einen Beitrag zur gemeinsamen Lageerfassung in Bezug auf Cyberbedrohungen und Sicherheitsvorfälle in den Mitgliedstaaten und – in Zusammenarbeit mit dem CERT-EU – bei den Einrichtungen der Union.

(9) Die ENISA arbeitet eng mit Europol, den CSIRTs und anderen einschlägigen nationalen Behörden zusammen, um die Abwehrbereitschaft im Bereich der Cybersicherheit und die Reaktion auf Ransomware-Vorfälle zu verbessern.

(10) Die ENISA trägt zur Einrichtung und Pflege eines europäischen Rahmens für die Cybersicherheitszertifizierung gemäß Titel III dieser Verordnung bei. Die ENISA fördert die Nutzung der europäischen Cybersicherheitszertifizierung, um der Fragmentierung des Binnenmarkts vorzubeugen.

(11) Die ENISA trägt zur Harmonisierung des digitalen Binnenmarkts bei, indem sie sich an Normungsarbeiten beteiligt, die für die Politik der Union im Bereich der Cybersicherheit relevant sind, und indem sie technische Spezifikationen entwickelt.

(12) Die ENISA fördert ein hohes Maß der Sensibilisierung für die Cybersicherheit bei Organisationen und Unternehmen.

Kapitel II
Aufgaben

Abschnitt 1
Unterstützung der Umsetzung der Unionspolitik und des Unionsrechts

Artikel 5
Unterstützung der Umsetzung der Unionspolitik und des Unionsrechts

(1) Die ENISA trägt zur Umsetzung der Unionspolitik und des Unionsrechts bei, indem sie

a) die Mitgliedstaaten dabei unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit kohärent umzusetzen, auch durch die Herausgabe technischer Leitlinien und Berichte, die Bereitstellung von Beratung und die Weitergabe bewährter Verfahren sowie durch die Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden in diesem Hinblick;

b) die Informationsweitergabe in und zwischen Sektoren, vor allem in Bezug auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Sektoren und Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) 2024/2847 fallen, durch die Bereitstellung von bewährten Verfahren und Leitfäden zu den verfügbaren Instrumenten und Verfahren unterstützt;

c) auf Ersuchen der Kommission die Mitgliedstaaten durch technische Leitlinien, unter anderem zu Maßnahmen zum Cybersicherheitsrisikomanagement, Instrumenten für die Bewertung des Cybersicherheitsreifegrads und Leitfäden für die Reaktion auf Sicherheitsvorfälle, die auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren zugeschnitten sind, oder bei der Umsetzung der Grundsätze der konzeptionsintegrierten Sicherheit für Produkte mit digitalen Elementen im Einklang mit der Verordnung (EU) 2024/2847 unterstützt, um die Verbesserung des Cybersicherheitsreifegrads und die Einhaltung des Unionsrechts im Bereich der Cybersicherheit zu erleichtern;

d) zur Arbeit der gemäß Artikel 14 Absatz 1 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe (im Folgenden „NIS-Kooperationsgruppe“), der gemäß Artikel 46e Absatz 1 der Verordnung (EU) Nr. 910/2014 eingesetzten europäischen Kooperationsgruppe für die digitale Identität, der in Artikel 90 der vorliegenden Verordnung genannten Europäischen Gruppe für die Cybersicherheitszertifizierung (im Folgenden „ECCG“) und der gemäß Artikel 52 Absatz 15 der Verordnung (EU) 2024/2847 eingesetzten Gruppe zur administrativen Zusammenarbeit (ADCO) beiträgt;

e) die Mitgliedstaaten und die einschlägigen Einrichtungen der Union bei der Entwicklung und Förderung von Strategien im Zusammenhang mit der Cybersicherheit unterstützt, die die allgemeine Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets bewahren;

f) gemäß der Verordnung (EU) 2024/2847 den Mitgliedstaaten und der Kommission technische Beratung und Unterstützung in Fragen im Zusammenhang mit der Durchführung der genannten Verordnung bereitstellt;

g) die Mitgliedstaaten bei der Amtshilfe und bei der Erleichterung solcher Kooperationsprozesse für wesentliche und wichtige Einrichtungen gemäß [Artikel 37a der Richtlinie (EU) 2022/2555] unterstützt;

h) auf Ersuchen des europäischen Datenschutzausschusses Beratung zur Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre bereitstellt.

(2) Die ENISA trägt zu den auf Unionsebene koordinierten Cybersicherheitsrisikobewertungen bei, einschließlich der gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchgeführten Bewertungen.

(3) Die ENISA gibt Leitlinien für die Interoperabilität der für die Informationsweitergabe verwendeten Netz- und Informationssysteme heraus, auch in Bezug auf grenzübergreifende Cyber-Hubs gemäß Artikel 6 Absatz 3 der Verordnung (EU) 2025/38.

(4) Die ENISA ist gemäß Artikel 14 Absatz 3 der Richtlinie (EU) 2022/2555 Mitglied der NIS-Kooperationsgruppe.

(5) Auf Ersuchen der Kommission stellt die ENISA Sachkenntnis, technische Beratung, Informationen oder Analysen zur Verfügung oder führt vorbereitende Arbeiten zu spezifischen Cybersicherheitsfragen durch, um die Politikgestaltung der Kommission und die Überwachung der Umsetzung der Rechtsvorschriften der Union zu unterstützen.

Artikel 6
Kapazitätsaufbau

Die ENISA unterstützt

1. die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Fähigkeiten bei der Bewältigung von Cyberbedrohungen und -vorfällen, indem sie ihnen Wissen und Sachkenntnis zur Verfügung stellt;

2. die Mitgliedstaaten auf deren Ersuchen bei der Aufstellung und Umsetzung von Strategien für eine Offenlegung von Schwachstellen auf freiwilliger Basis;

3. im Einklang mit der Verordnung (EU, Euratom) 2023/2841 den CERT-EU und den Interinstitutionellen Cybersicherheitsbeirat in ihren Bemühungen, den Einrichtungen der Union bei der Stärkung ihrer Cybersicherheit zu helfen und die Prävention, Erkennung und Analyse von Cyberbedrohungen und -vorfällen sowie ihre Fähigkeiten zur Reaktion auf solche Cyberbedrohungen und -vorfälle zu verbessern;

4. die Mitgliedstaaten auf deren Ersuchen beim Aufbau nationaler CSIRTs nach Artikel 10 Absatz 10 der Richtlinie (EU) 2022/2555;

5. die Mitgliedstaaten auf deren Ersuchen bei der Ausarbeitung oder Aktualisierung nationaler Cybersicherheitsstrategien und wesentlicher Leistungsindikatoren nach Artikel 7 Absatz 4 der Richtlinie (EU) 2022/2555,

fördert die unionsweite Verbreitung dieser Strategien und stellt die Fortschritte bei deren Umsetzung in der gesamten Union fest, um bewährte Verfahren bekannt zu machen;

6. die Organe der Union auf deren Ersuchen bei der Ausarbeitung und Überprüfung von Unionsstrategien zur Cybersicherheit, fördert deren Verbreitung und verfolgt die Fortschritte bei deren Umsetzung;

7. die CSIRTs der Mitgliedstaaten bei der Anhebung des Niveaus ihrer Fähigkeiten, auch durch die Förderung des Dialogs und Informationsaustauschs, damit jedes CSIRT entsprechend dem Stand der Technik einen gemeinsamen Bestand an Minimalfähigkeiten hat und entsprechend der bewährten Praxis arbeitet;

8. die Mitgliedstaaten, die Einrichtungen der Union sowie öffentliche und private Interessenträger in ihren Bemühungen um die Bewertung, den Ausbau und die Verbesserung der Fachkräftebasis im Bereich Cybersicherheit, unter anderem durch die Entwicklung, Pflege und Förderung der Verbreitung einschlägiger Instrumente wie des ECSF und der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Abschnitt 4 dieses Kapitels;

9. einschlägige öffentliche Stellen sowie private Interessenträger, indem sie, gegebenenfalls in Zusammenarbeit mit Interessenträgern, gezielte Fortbildungen für sie durchführt;

10. die NIS-Kooperationsgruppe beim Austausch von bewährten Verfahren und Informationen, insbesondere im Zusammenhang mit der Umsetzung der Richtlinie (EU) 2022/2555 gemäß Artikel 14 Absatz 4 Buchstabe c der genannten Richtlinie;

11. die gemäß der Verordnung (EU) 2024/2847 benannten Marktüberwachungsbehörden bei ihren Tätigkeiten zur Gewährleistung der wirksamen Durchführung der genannten Verordnung, einschließlich der Unterstützung von Leitlinien und technischer Beratung für Wirtschaftsteilnehmer, der Unterstützung von Konformitätsprüfungen, der Bewertung von Risiken, gemeinsamen Tätigkeiten und koordinierten Kontrollen (Sweeps) gemäß der Verordnung (EU) 2024/2847;

12. die Mitglieder der ECCG beim Austausch bewährter Verfahren und auf Ersuchen einzelner Mitgliedstaaten die nationalen Behörden für die Cybersicherheitszertifizierung bei der Umsetzung der europäischen Systeme für die Cybersicherheitszertifizierung auf nationaler Ebene;

13. Behörden und private Interessenträger im Zusammenhang mit Konformitätsbewertungs- und allgemeinen Bewertungstätigkeiten, einschließlich Konformitätsbewertungsstellen und kleiner und mittlerer Unternehmen, um ein robustes, wettbewerbsfähiges, inklusives und harmonisiertes Ökosystems für die Konformitätsbewertung zu fördern, das der Durchführung der Verordnung (EU) 2024/2847 und des europäischen Rahmens für die Cybersicherheitszertifizierung dient;

14. das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und das Netzwerk nationaler Koordinierungszentren, die gemäß der Verordnung (EU) 2021/887 eingerichtet wurden, durch die Weitergabe von Informationen über aktuelle und neu

auftretende Risiken und Cyberbedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnologien;

15. die Mitgliedstaaten durch die Bereitstellung technischer Unterstützung, unter anderem für die Einrichtung und den Betrieb von Reallaboren im Bereich der Cybersicherheit im Einklang mit den einschlägigen Rechtsvorschriften der Union.

Artikel 7
Sensibilisierung und Talentpool

Die ENISA unterstützt die Mitgliedstaaten bei ihren Bemühungen um die Sensibilisierung für die Politik und die Rechtsvorschriften der Union im Bereich der Cybersicherheit und die Förderung von deren Sichtbarkeit, indem sie praktisch anwendbare Instrumente und Leitlinien entwickelt. Die ENISA unterstützt Initiativen zum Ausbau des europäischen Talentpools im Bereich der Cybersicherheit, insbesondere durch die Koordinierung von Auswahlverfahren.

Artikel 8
Marktkenntnis und -analysen

(1) Die ENISA führt Analysen der wichtigsten Markttrends auf dem Cybersicherheitsmarkt sowohl auf der Nachfrage- als auch auf der Angebotsseite durch, insbesondere im Zusammenhang mit den Bereichen, in denen europäische Systeme für die Cybersicherheitszertifizierung bestehen oder geplant sind, in den in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren und den unter die Verordnung (EU) 2024/2847, einschließlich der Anhänge III und IV der genannten Verordnung, fallenden Produktkategorien, und verbreitet diese.

(2) Die ENISA führt Analysen der Trends in der Cybersicherheitstechnik durch, insbesondere in Bezug auf Tätigkeiten und Einrichtungen, die in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallen, und Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) 2024/2847 fallen, und verbreitet diese.

(3) Die ENISA baut Wissen auf und verbreitet technische Empfehlungen und Analysen zu modernsten Instrumenten, Rahmen, Normen und bewährten Verfahren im Bereich der Cybersicherheit.

Artikel 9
Internationale Zusammenarbeit

Die ENISA unterstützt die Bemühungen der Union um Zusammenarbeit mit Drittländern und internationalen Organisationen sowie innerhalb der einschlägigen Rahmen für internationale Zusammenarbeit, um die internationale Zusammenarbeit in Angelegenheiten der Cybersicherheit zu fördern, indem sie

a) soweit zweckmäßig, bei der Organisation von internationalen Übungen als Beobachterin mitwirkt, die Ergebnisse solcher Übungen analysiert und sie dem Verwaltungsrat vorlegt;

b) auf Ersuchen der Kommission den Austausch bewährter Verfahren mit Drittländern und internationalen Organisationen erleichtert;

c) der Kommission auf deren Ersuchen mit Sachkenntnis zur Seite steht;

d) die Kommission bei Fragen zur internationalen Anerkennung europäischer Cybersicherheitszertifikate gemäß Artikel 87 fachlich berät und unterstützt;

e) die Kommission in Zusammenarbeit mit der nach Artikel 90 eingesetzten ECCG bei Fragen der internationalen Normung und gegebenenfalls beim Umgang mit den einschlägigen internationalen Normungsgremien fachlich berät und unterstützt.

Abschnitt 2

Operative Zusammenarbeit

Artikel 10
Operative Zusammenarbeit auf Unionsebene

(1) Die ENISA unterstützt die operative Zusammenarbeit der Mitgliedstaaten und Einrichtungen der Union untereinander (über den CERT-EU) und zwischen anderen Beteiligten.

(2) Die ENISA ist Mitglied des gemäß Artikel 15 Absatz 1 der Richtlinie (EU) 2022/2555 eingerichteten Netzwerks nationaler CSIRTs und nimmt die Sekretariatsgeschäfte des CSIRTs-Netzwerks gemäß Artikel 15 Absatz 2 der Richtlinie (EU) 2022/2555 wahr.

(3) Die ENISA nimmt die Sekretariatsgeschäfte des Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) gemäß Artikel 16 Absatz 2 Unterabsatz 2 der Richtlinie (EU) 2022/2555 wahr.

(4) Die ENISA unterstützt die technische und operative Zusammenarbeit zwischen den Mitgliedstaaten insbesondere über das CSIRTs-Netzwerk und das EU-CyCLONe. Diese Unterstützung umfasst Folgendes:

a) Beratung dazu, wie Fähigkeiten zur Verhinderung, und Aufdeckung von Sicherheitsvorfällen, zur Reaktion darauf und zur Wiederherstellung danach verbessert werden können;

b) auf Ersuchen eines oder mehrerer Mitgliedstaaten Bereitstellung von Beratung und Bewertungen in Bezug auf einen bestimmten potenziellen oder andauernden Sicherheitsvorfall bzw. eine entsprechende Cyberbedrohung, auch durch die Bereitstellung von Sachkenntnis und die Erleichterung der technischen Bewältigung solcher Vorfälle sowie durch die Unterstützung der freiwilligen Weitergabe einschlägiger Informationen und technischer Lösungen zwischen den Mitgliedstaaten;

c) Analyse von Schwachstellen, Bedrohungen und Sicherheitsvorfällen;

d) auf Ersuchen eines oder mehrerer Mitgliedstaaten Unterstützung in Bezug auf nachträgliche technische Untersuchungen von erheblichen Sicherheitsvorfällen im Sinne des Artikel 23 Absatz 3 der Richtlinie (EU) 2022/2555;

e) Beitrag zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Cybersicherheitskrisen auf operativer Ebene, insbesondere durch Unterstützung des EU-CyCLONe bei der Erstellung von Berichten an die politische Ebene und durch Erleichterung der

zeitnahen Informationsweitergabe zwischen dem CSIRTs-Netzwerk und dem EU-CyCLONe;

(5) Auf Ersuchen eines Mitgliedstaats oder einer Einrichtung der Union in Zusammenarbeit mit dem CERT-EU unterstützt die ENISA eine kohärente öffentliche Kommunikation über einen Sicherheitsvorfall oder eine Cyberbedrohung.

(6) Die ENISA unterstützt die Zusammenarbeit zwischen den Mitgliedstaaten und über den CERT-EU zwischen den Einrichtungen der Union im Hinblick auf den Einsatz sicherer Kommunikationsinstrumente. Die ENISA verwendet innerhalb des CSIRTs-Netzwerks und des EU-CyCLONe sichere Kommunikationsinstrumente, die von Rechtsträgern bereitgestellt werden, die in der Union niedergelassen sind bzw. als in der Union niedergelassen gelten und von Mitgliedstaaten oder von Staatsangehörigen der Mitgliedstaaten kontrolliert werden.

Artikel 11
Gemeinsame Lageerfassung im Bereich der Cybersicherheit

(1) Für die Zwecke einer besseren gemeinsamen Lageerfassung in Bezug auf Cyberbedrohungen und -vorfälle in den Mitgliedstaaten und bei Einrichtungen der Union wird die ENISA

a) in Zusammenarbeit mit dem EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission, dem CERT-EU, Europol und anderen einschlägigen Einrichtungen der Union Ablagen verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen entwickeln, einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren;

b) gemäß Artikel 12 Frühwarnungen in Bezug auf einen potenziellen oder andauernden erheblichen Sicherheitsvorfall oder Sicherheitsvorfall großen Ausmaßes oder eine potenziell grenzübergreifende Cyberbedrohung abgeben, insbesondere in Bezug auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren;

c) auf Ersuchen des CSIRTs-Netzwerks, des EU-CyCLONe oder der Kommission zeitnahe Ad-hoc-Analysen zu sich abzeichnenden Trends bei Sicherheitsvorfällen vorlegen;

d) auf Ersuchen der Mitgliedstaaten oder der Kommission Analysen oder andere Informationen über ein tatsächliches oder wahrgenommenes Cybersicherheitsrisiko oder eine tatsächliche oder wahrgenommene Cybersicherheitsbedrohung bereitstellen;

e) Analysen und technische Beratung zu Cybersicherheitsrisiken bei Produkten mit digitalen Elementen bereitstellen, auch zur Unterstützung der Marktüberwachung und durch die Erstellung eines zweijährlichen technischen Berichts über aufkommende Trends gemäß Artikel 17 Absatz 3 der Verordnung (EU) 2024/2847;

f) regelmäßig einen eingehenden technischen EU-Cybersicherheitslagebericht über Sicherheitsvorfälle und Cyberbedrohungen erstellen und diesen dem Rat, EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission, dem Europäischen Auswärtigen Dienst und Europol zur Verfügung stellen;

g) Trends bei Techniken, Forderungen und Auswirkungen von Ransomware-Angriffen beobachten und der Kommission, dem CSIRTs-Netzwerk sowie dem

EU-CyCLONe und Europol Informationen über diese Trends zur Verfügung stellen.

(2) Für die Zwecke einer besseren gemeinsamen Lageerfassung in Bezug auf Cyberbedrohungen und -vorfälle bei den Interessenträgern wird die ENISA

a) Analysen von Cyberbedrohungen, Sicherheitsvorfällen, Trends, neu aufkommender Technik und deren Auswirkungen durchführen, einschließlich einer regelmäßigen Analyse der in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren und der einschlägigen Produktkategorien, die unter die Verordnung (EU) 2024/2847 fallen;

b) in Zusammenarbeit mit der Kommission und gegebenenfalls dem CSIRTs-Netzwerk Beratung, Leitlinien und bewährte Verfahren für die Sicherheit der Netz- und Informationssysteme bereitstellen, vor allem für die Sicherheit der Infrastrukturen, die die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren unterstützen;

c) langfristige strategische Analysen der Cyberbedrohungen und -vorfälle durchführen, um neu auftretende Trends zu erkennen und zur Verhinderung von Sicherheitsvorfällen beizutragen.

(3) Die ENISA kann die in Absatz 2 genannten Analysen, Ratschläge, Leitlinien, bewährten Verfahren und Berichte im Einvernehmen mit den in Absatz 2 genannten beitragenden Einrichtungen veröffentlichen.

(4) Bei der Durchführung der in Absatz 1 Buchstaben a bis d und Buchstabe f sowie Absatz 2 aufgeführten Tätigkeiten stützt sich die ENISA auf ihre eigenen Analysen und gegebenenfalls auf die Informationen, die sie bei der Wahrnehmung ihrer Aufgaben erhält, darunter

a) Informationen aus öffentlich zugänglichen Quellen, einschließlich öffentlich bekannter Schwachstellen in IKT-Produkten oder -Diensten, die in der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank enthalten sind;

b) Informationen, die von Mitgliedstaaten, Einrichtungen der Union, dem CERT-EU, Partnern aus dem Privatsektor oder nichtstaatlichen Partnern sowie Drittländern und internationalen Organisationen weitergegeben werden, vorbehaltlich etwaiger Beschränkungen der Weiterverbreitung dieser Informationen durch sichtbare Kennzeichnungen.

(5) Die ENISA arbeitet bei der Ausarbeitung des in Absatz 1 Buchstabe e genannten eingehenden technischen EU-Cybersicherheitslageberichts über Sicherheitsvorfälle und Cyberbedrohungen eng mit den Mitgliedstaaten zusammen. Der Bericht beruht auf öffentlich zugänglichen Informationen, eigenen Analysen der ENISA und Berichten, die ihr unter anderem von den CSIRTs der Mitgliedstaaten oder den mit der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstellen (in beiden Fällen auf freiwilliger Basis) sowie dem EC3 und dem CERT-EU übermittelt werden. Im Einvernehmen mit den beitragenden Einrichtungen kann die ENISA eine aggregierte Fassung des Berichts öffentlich zugänglich machen.

Artikel 12
Frühwarnungen

(1) Frühwarnungen gemäß Artikel 11 Absatz 1 Unterabsatz 1 Buchstabe b dieser Verordnung enthalten einschlägige Informationen über einen potenziellen oder andauernden erheblichen Sicherheitsvorfall oder Sicherheitsvorfall großen Ausmaßes oder eine potenzielle grenzübergreifende Cyberbedrohung, insbesondere in Bezug auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren. Dazu können Informationen über öffentlich bekannte Schwachstellen und Angaben darüber, ob sie Produkte mit digitalen Elementen betreffen, die unter die Verordnung (EU) 2024/2847 fallen, über Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen und Empfehlungen zu Risikominderungsmaßnahmen gehören.

(2) Frühwarnungen gemäß Artikel 11 Absatz 1 Unterabsatz 1 Buchstabe b werden so bald wie möglich dem/den betreffenden CSIRT(s) und gegebenenfalls dem CSIRTs-Netzwerk und dem EU-CyCLONe übermittelt.

(3) Die ENISA bietet Einrichtungen, die in den in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren tätig sind, einen Frühwarndienst.

(4) Der in Absatz 3 genannte Dienst wird auf Ersuchen der Einrichtung und in einem maschinenlesbaren Format, das öffentlich zugänglich gemacht wird, erbracht. Dieser Dienst umfasst die Weitergabe von Informationen über Indikatoren für Cyberbedrohungen und Empfehlungen zu Risikominderungsmaßnahmen.

(5) Die ENISA legt ein Verfahren zur Verbreitung der Frühwarnungen an die in Absatz 3 genannten Einrichtungen fest.

Artikel 13
Unterstützung bei der Reaktion auf Sicherheitsvorfälle und Überprüfung

(1) Die ENISA betreibt und verwaltet ganz oder teilweise die EU-Cybersicherheitsreserve gemäß der Verordnung (EU) 2025/38.

(2) Auf Ersuchen der Kommission oder des EU-CyCLONe nimmt die ENISA mit Unterstützung des CSIRTs-Netzwerks und mit Zustimmung der betroffenen Mitgliedstaaten eine Überprüfung und Bewertung schwerwiegender Cybersicherheitsvorfälle oder von Cybersicherheitsvorfällen großen Ausmaßes im Einklang mit Artikel 21 der Verordnung (EU) 2025/38 vor.

(3) Die ENISA unterstützt in Zusammenarbeit mit Europol und den CSIRTs oder gegebenenfalls anderen zuständigen Behörden einzelne wesentliche und wichtige Einrichtungen, die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführt sind, bei der Vorbereitung und Reaktion auf Ransomware-Vorfälle sowie bei der Wiederherstellung danach. Dazu richtet die ENISA einen Helpdesk ein und nutzt insbesondere die bessere gemeinsame Lageerfassung in Bezug auf Cyberbedrohungen und -vorfälle gemäß Artikel 11 Absatz 1 Unterabsatz 1 Buchstaben a und g dieser Verordnung.

Artikel 14
Cybersicherheitsübungen auf Unionsebene

(1) Die ENISA unterstützt die Kommission bei der Erstellung eines jährlichen fortlaufenden Programms von Cybersicherheitsübungen auf Unionsebene.

(2) Die ENISA unterhält eine Ablage der aus den in Absatz 1 genannten Übungen gewonnenen Erkenntnisse und gibt den Mitgliedstaaten und gegebenenfalls den Einrichtungen der Union Empfehlungen dazu, wie die gewonnenen Erkenntnisse wirksam und effizient genutzt werden können.

(3) Auf Ersuchen des EU-CyCLONe und/oder der Kommission organisiert die ENISA Cybersicherheitsübungen auf Unionsebene, einschließlich Tests der Abwehrbereitschaft zur Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen auf Unionsebene, oder trägt zur Organisation solcher Übungen bei.

(4) Auf Ersuchen der Mitgliedstaaten unterstützt die ENISA diese bei der Organisation nationaler Cybersicherheitsübungen.

(5) Auf Ersuchen des CERT-EU trägt die ENISA zur Organisation von Cybersicherheitsübungen bei, die der CERT-EU gemäß Artikel 13 Absatz 7 der Verordnung (EU, Euratom) 2023/2841 organisiert.

Artikel 15
Bereitstellung von Instrumenten und Plattformen

(1) Die ENISA sorgt für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung operativer technischer Instrumente einschließlich Plattformen für die Cybersicherheit auf Unionsebene, insbesondere der gemäß Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 eingerichteten einheitlichen Meldeplattform [und der gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstelle zur Meldung von Vorfällen], sowie von Testinstrumenten zur Unterstützung der Durchführung von Konformitätsbewertungsverfahren im Einklang mit den einschlägigen Rechtsvorschriften der Union.

(2) Soweit angebracht arbeitet die ENISA für die Zwecke des Absatzes 1 mit dem CSIRTs-Netzwerk und gegebenenfalls den Marktüberwachungsbehörden zusammen und tauscht Informationen mit ihnen aus.

Artikel 16
Schwachstellenmanagementdienste

Die ENISA entwickelt einen gemeinsamen Schwachstellenmanagementdienst der Union und stellt Interessenträgern Schwachstellenmanagementdienste bereit, indem sie

a) die gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichtete europäische Schwachstellendatenbank pflegt;

b) Schwachstellenmanagementdienste für Interessenträger bereitstellt, aufbauend auf der europäischen Schwachstellendatenbank und unter Rückgriff auf die der ENISA zur Verfügung stehenden einschlägigen Informationen;

c) gegebenenfalls eine strukturierte Zusammenarbeit mit Organisationen aufnimmt, die ähnliche Programme, Register oder Datenbanken wie die europäische Schwachstellendatenbank bereitstellen;

d) die gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 als Koordinatoren benannten CSIRTs im Hinblick auf die Steuerung der koordinierten Offenlegung von Schwachstellen, die erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten nach sich ziehen könnten, aktiv unterstützt;

e) in Zusammenarbeit mit den zuständigen nationalen Behörden, den CSIRTs, der Branche und der Forschungsgemeinschaft Methoden und Governance-Mechanismen für die Ermittlung und koordinierte Offenlegung von Schwachstellen entwickelt und aufrechterhält.

Abschnitt 3

Cybersicherheitszertifizierung und Normung

Artikel 17
Cybersicherheitszertifizierung

(1) Die ENISA trägt zur Entwicklung und Umsetzung der Unionspolitik auf dem Gebiet der Cybersicherheitszertifizierung, wie in Titel III dieser Verordnung festgelegt, bei und fördert diese. Die ENISA ist zuständig für

a) die Ausarbeitung möglicher europäischer Systeme für die Cybersicherheitszertifizierung (im Folgenden „mögliche Systeme“) für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und die Cyberabwehr von Einrichtungen gemäß Artikel 74 und gegebenenfalls technischer Spezifikationen gemäß Artikel 77;

b) die Pflege der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 75, auch im Hinblick auf eine mögliche Überprüfung der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 76;

c) die Förderung der Einführung angenommener Systeme und die Pflege einer eigenen Website mit Informationen über europäische Systeme für die Cybersicherheitszertifizierung, europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen gemäß Artikel 79 und deren Bekanntmachung;

d) die Organisation des Kapazitätsaufbaus im Zusammenhang mit Zertifizierungsverfahren, Bewertungstätigkeiten, gegenseitigen Begutachtungen und gegenseitigen Bewertungen, unter anderem durch Unterstützung der Mitgliedstaaten auf deren Ersuchen gemäß Artikel 6 Nummer 12.

(2) Die ENISA unterstützt die Kommission bei den folgenden Tätigkeiten:

a) Führung der ECCG gemäß Artikel 90;

b) Organisation einer europäischen Versammlung für die Cybersicherheitszertifizierung gemäß Artikel 72 Absatz 1;

c) Tätigkeiten in Verbindung mit der internationalen Anerkennung europäischer Cybersicherheitszertifikate gemäß Artikel 87;

d) Organisation gegenseitiger Begutachtungen gemäß Artikel 89;

e) Ausarbeitung von Musterbestimmungen, auf die in den europäischen Systemen für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten und der Cyberabwehr von Einrichtungen gemäß Artikel 81 Absatz 5 Bezug zu nehmen ist.

Artikel 18
Normung, technische Spezifikationen und Leitlinien

(1) Die ENISA arbeitet technische Spezifikationen und Leitlinien aus, um die Umsetzung der Rechtsvorschriften der Union im Bereich der Cybersicherheit zu unterstützen. Dabei berücksichtigt die ENISA bestehende europäische und internationale Normen sowie sonstige einschlägige technische Spezifikationen. Die ENISA sorgt für die Kohärenz ihrer technischen Spezifikationen und Leitlinien.

(2) Die ENISA beobachtet die Entwicklung der Normung auf Unionsebene und – im Einklang mit Artikel 9 – auf internationaler Ebene, beteiligt sich gegebenenfalls daran und steuert sie, um die Politik der Union im Bereich der Cybersicherheit zu unterstützen.

(3) Die ENISA unterstützt die Entwicklung und Bewertung kryptografischer Algorithmen. Bewertet die ENISA einen kryptografischen Algorithmus positiv, so arbeitet sie im Einklang mit der Verordnung (EU) Nr. 1025/2012 mit den europäischen Normungsgremien zusammen, um dessen Normung zu unterstützen.

(4) Die ENISA berät die Kommission und gegebenenfalls die Mitgliedstaaten in technischen Fragen zu geeigneten Normen oder technischen Spezifikationen zur Unterstützung der Unionspolitik im Bereich der Cybersicherheit, einschließlich der Harmonisierungsrechtsvorschriften der Union im Bereich der Cybersicherheit, insbesondere der Verordnung (EU) 2024/2847, der technischen Bereiche für die Zwecke des Artikels 25 der Richtlinie (EU) 2022/2555 und der europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 81 Absatz 1 Buchstabe d.

(5) Die ENISA unterstützt die Kommission bei der Bewertung der Entwürfe harmonisierter Normen, um die Umsetzung der Harmonisierungsrechtsvorschriften der Union im Bereich der Cybersicherheit zu fördern.

(6) Die ENISA fördert die Übernahme europäischer und internationaler Normen für Cybersicherheit.

(7) Die ENISA nimmt die in den Absätzen 1 bis 6 genannten Aufgaben mit Integrität, unparteiisch und vertraulich wahr und kann dazu bestimmten technischen Stellen ihre Berechtigung zur Mitarbeit entziehen oder diese aussetzen, wenn eine solche Mitarbeit anderen Aufgaben oder Zielen zuwiderläuft.

Abschnitt 4
Einrichtung der Akademie für Cybersicherheitskompetenzen

Artikel 19
Europäischer Kompetenzrahmen für Cybersicherheit

(1) Die ENISA entwickelt einen europäischen Kompetenzrahmen für Cybersicherheit (ECSF) und macht ihn öffentlich zugänglich. Vor der Veröffentlichung oder Aktualisierung des ECSF gemäß Absatz 4 konsultiert die ENISA die Kommission.

(2) Im ECSF werden Profile von Cybersicherheitsfachkräften und die Zuordnung bestimmter Aufgaben, Fähigkeiten und Kenntnisse zu einem bestimmten Rollenprofil festgelegt. Die Verwendung des ECSF ist für öffentliche und private Einrichtungen freiwillig.

(3) Die ENISA kann bei der Entwicklung und Einführung des ECSF Interessenträger konsultieren.

(4) Die ENISA prüft regelmäßig, ob der ECSF aktualisiert werden muss, und aktualisiert ihn gegebenenfalls.

Artikel 20

Entwicklung, Annahme und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen

(1) Die ENISA ist für die Entwicklung, Annahme und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen zuständig. Die Verwendung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen ist für nationale öffentliche Stellen und private Einrichtungen freiwillig, sofern im nationalen Recht nichts anderes bestimmt ist.

(2) Vor der Einführung eines neuen Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen konsultiert die ENISA die Kommission. Die ENISA darf ein solches System erst nach einer befürwortenden Stellungnahme der Kommission annehmen. Bei der Ausarbeitung eines Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen kann die ENISA einschlägige Interessenträger konsultieren.

(3) Ein System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen umfasst Folgendes:

a) Gegenstand und Anwendungsbereich des Bescheinigungssystems auf der Grundlage der ECSF-Rollenprofile oder von Teilsätzen davon;

b) Anforderungen an Einzelpersonen, die gemäß Artikel 21 für die Durchführung von Bewertungen ausgebildet sind (im Folgenden „Prüfer“), die erforderlichen Fähigkeiten, Kenntnisse und Erfahrungen sowie Ausbildungsmethoden;

c) Analyse der Marktakzeptanz für jedes Bescheinigungssystem;

d) gewonnene Erkenntnisse, Bewertungsmethoden und Bedingungen, die befugte Bescheinigungsanbieter anwenden müssen, um den Nachweis der erforderlichen Kompetenzen durch eine Einzelperson gemäß Artikel 21 zu bewerten;

e) gegebenenfalls eine oder mehrere Kompetenzniveaus;

f) Vorschriften über die Aufbewahrung von Aufzeichnungen durch befugte Bescheinigungsanbieter;

g) Inhalt und Format der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen unter gebührender Berücksichtigung von Artikel 21 Absatz 5 Buchstabe e;

h) die maximale Gültigkeitsdauer einer nach dem Bescheinigungssystem ausgestellten europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen.

(4) Ein System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen kann die Deckung der voraussichtlichen Kosten einer europäischen Einzelbescheinigung von Cybersicherheitskompetenzen vorsehen.

(5) Die ENISA sorgt während der gesamten Ausarbeitung der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen für eine enge Zusammenarbeit mit den Mitgliedstaaten.

(6) Die Änderung eines Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen berührt nicht die gemäß Artikel 22 Absatz 3 Buchstabe a erteilte Befugnis, die für den Zeitraum gültig bleibt, für den sie erteilt wird.

Artikel 21
Befugte Bescheinigungsanbieter

(1) Befugte Bescheinigungsanbieter bewerten, ob Einzelpersonen die Anforderungen eines Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen erfüllen, und stellen, wenn diese Anforderungen erfüllt sind, europäische Einzelbescheinigungen von Cybersicherheitskompetenzen aus. Bescheinigungsanbieter können mehrere Befugnisse haben, die jeweils für ein System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen erteilt werden.

(2) Die ENISA stellt den Prüfern Orientierungshilfen bereit und führt obligatorische Fortbildungen für Prüfer zu den Anforderungen und Bewertungsmethoden durch, die in dem in Artikel 20 Absatz 3 Buchstabe b genannten System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen enthalten sind.

(3) Einrichtungen, die befugte Bescheinigungsanbieter werden oder ihre Befugnis verlängern lassen möchten (im Folgenden „Antragsteller“), stellen einen Antrag bei der ENISA. Sie müssen folgende Anforderungen erfüllen:

a) Sie müssen Rechtspersönlichkeit besitzen;

b) sie müssen in der Lage sein, die in dieser Verordnung festgelegten Aufgaben im Zusammenhang mit Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen wahrzunehmen, gleichgültig, ob die Bewertung von dem befugten Bescheinigungsanbieter selbst, in seinem Auftrag oder unter seiner Verantwortung durchgeführt wird;

c) ihnen müssen die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben zur Verfügung stehen, die mit dem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen verbunden sind, und sie müssen Zugang zu allen benötigten Ausrüstungen oder Einrichtungen haben.

Für die Zwecke von Unterabsatz 1 Buchstabe b ist jegliche Unterauftragsvergabe oder die Inanspruchnahme von externem Personal angemessen zu dokumentieren, darf nicht über Vermittler erfolgen und bedarf einer schriftlichen Vereinbarung, in der unter anderem Vertraulichkeitsaspekte und Interessenkonflikte geregelt werden.

(4) Die Antragsteller dürfen keine Hochrisikoanbieter sein.

(5) Befugte Bescheinigungsanbieter müssen die folgenden Pflichten erfüllen:

a) für die Umsetzung jedes Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen:

i) Sie müssen über die erforderlichen Prüfer und Mitarbeitenden verfügen, um ihre in dem System festgelegten Tätigkeiten zeitnah durchführen zu können,

ii) sie müssen sicherstellen, dass die Prüfer das Berufsgeheimnis wahren, unparteiisch sind und ihre Arbeit unabhängig und mit höchster beruflicher Integrität ausführen,

iii) sie müssen über schriftlich niedergelegte Verfahren für die Durchführung ihrer Tätigkeiten im Rahmen des Systems verfügen, für das sie befugt sind;

b) sie dürfen ihre eigenen Prüfer nicht bewerten und ihnen keine europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen ausstellen;

c) sie müssen gegebenenfalls durch Schaffung geeigneter Schutzvorkehrungen sicherstellen, dass ihre Prüfer ihre Arbeit unabhängig ausführen können, insbesondere wenn diese Einzelpersonen zu ihrer eigenen Struktur gehören oder Beschäftigte oder Auszubildende einer solchen Struktur sind;

d) sie dürfen sich nicht mit Tätigkeiten befassen, die die Unabhängigkeit bei der Beurteilung oder die Integrität ihrer Prüfer beeinträchtigen können;

e) sie müssen sicherstellen, dass elektronische Einzelbescheinigungen der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen auf Ersuchen einer Einzelperson als elektronische Attributsbescheinigungen in einem Format ausgestellt werden, das in den europäischen Brieftaschen für die digitale Identität gemäß der Verordnung (EU) Nr. 910/2014 gespeichert werden kann.

(6) Befugte Bescheinigungsanbieter unterrichten die ENISA unverzüglich, wenn die in den Absätzen 3 und 4 aufgeführten Anforderungen oder die in Absatz 5 aufgeführten Verpflichtungen nicht mehr erfüllt werden oder wenn Zweifel an der Erfüllung dieser Anforderungen oder Verpflichtungen bestehen, auch in Bezug auf die Unabhängigkeit der Prüfer.

(7) Befugte Bescheinigungsanbieter können von Einzelpersonen eine Gebühr für die Bewertung und Ausstellung der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen verlangen, wobei die voraussichtlichen Kosten einer europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Artikel 20 Absatz 4 zu berücksichtigen sind, die auf einer eigenen Website gemäß Artikel 23 Buchstabe d veröffentlicht werden.

(8) Antragsteller und befugte Bescheinigungsanbieter erlauben der ENISA, im Rahmen des Antragsverfahrens oder der Aufrechterhaltung der Befugnis Bewertungen durchzuführen und alle einschlägigen Informationen weiterzugeben, um sicherzustellen, dass die in den Absätzen 3 und 4 festgelegten Anforderungen oder die in Absatz 5 festgelegten Verpflichtungen gemäß Artikel 22 Absatz 2 (weiterhin) erfüllt werden.

Artikel 22
Prüfung von Anträgen auf Zulassung als befugter Bescheinigungsanbieter und Aufrechterhaltung von Befugnissen

(1) Die Antragsteller entrichten für die Prüfung ihres Antrags eine Gebühr an die ENISA. Befugte Bescheinigungsanbieter zahlen eine Gebühr für die Aufrechterhaltung ihrer Befugnis an die ENISA.

(2) Die ENISA bewertet, ob die in Artikel 21 Absätze 3 und 4 festgelegten Anforderungen und die in Artikel 21 Absatz 5 festgelegten Verpflichtungen von Antragstellern und befugten Bescheinigungsanbietern (weiterhin) erfüllt werden.

(3) Nach der Prüfung des Antrags anhand der Anforderungen gemäß Artikel 21 Absätze 3 und 4 kann die ENISA eine der folgenden Entscheidungen treffen:

a) Erteilung oder Verlängerung des Status eines befugten Bescheinigungsanbieters;

b) Ablehnung der Zulassung oder Verlängerung der Zulassung als befugter Bescheinigungsanbieter;

c) Abschluss Antragsbearbeitung wegen Untätigkeit des Antragstellers nach Anforderung zusätzlicher Informationen durch die ENISA.

Die ENISA kann solche Entscheidungen auf der Grundlage ihrer Bewertung gemäß Artikel 22 Absatz 2 oder in dem in Artikel 21 Absatz 6 genannten Fall ändern, aussetzen oder widerrufen.

(4) Die ENISA trifft die in Absatz 3 genannte Entscheidung innerhalb von drei Monaten nach dem Tag der Einreichung eines Antrags gemäß Artikel 21 Absatz 3. Hat die ENISA vom Antragsteller zusätzliche Informationen angefordert, so trifft sie die in Absatz 3 genannte Entscheidung innerhalb eines Monats nach Eingang der zusätzlichen Informationen.

(5) Die in Absatz 3 Buchstabe a genannte Entscheidung gilt für höchstens drei Jahre und enthält die Angabe der Gebühr für die jährliche Aufrechterhaltung der Befugnis.

(6) Die ENISA stellt sicher, dass ihre Tätigkeiten im Zusammenhang mit der Entwicklung und Annahme von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Artikel 20 streng getrennt sind und unabhängig von den Tätigkeiten zur Prüfung von Anträgen und zu Bewertungen gemäß den Absätzen 2 und 3 durchgeführt werden.

Artikel 23
Information der Öffentlichkeit

Die ENISA unterhält und aktualisiert regelmäßig eine eigene Website mit öffentlichen Informationen über

a) den ECSF, einschließlich des Rahmens und des Zeitplans für die Aktualisierung;

b) die Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, deren Fortschritte und Zeitpläne für die weitere Entwicklung;

c) die Gebühren im Zusammenhang mit jedem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, das gemäß Artikel 47 dieser Verordnung angenommen wird;

d) die voraussichtlichen Kosten einer europäischen Einzelbescheinigung von Cybersicherheitskompetenzen gemäß Artikel 20 Absatz 4;

e) die Liste befugter Bescheinigungsanbieter.

Kapitel III
Organisation der ENISA

Artikel 24
Verwaltungs- und Leitungsstruktur der ENISA

Die Verwaltungs- und Leitungsstruktur der ENISA umfasst

a) einen Verwaltungsrat, der die in Artikel 28 vorgesehenen Aufgaben wahrnimmt,

b) einen Exekutivrat, der die in Artikel 30 vorgesehenen Aufgaben wahrnimmt,

c) einen Exekutivdirektor, der die in Artikel 32 genannten Zuständigkeiten wahrnimmt,

d) einen stellvertretenden Exekutivdirektor, der die in Artikel 34 genannten Zuständigkeiten wahrnimmt,

e) eine ENISA-Beratungsgruppe,

f) eine Beschwerdekammer, die die in den Artikeln 39 bis 42 vorgesehenen Aufgaben wahrnimmt.

Abschnitt 1
Verwaltungsrat

Artikel 25
Zusammensetzung des Verwaltungsrats

(1) Dem Verwaltungsrat gehören je ein von jedem Mitgliedstaat ernanntes Mitglied und zwei von der Kommission ernannte Mitglieder an. Alle Mitglieder haben Stimmrecht.

(2) Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter. Die Stellvertreter vertreten die Mitglieder in deren Abwesenheit.

(3) Jeder Mitgliedstaat ernennt den Leiter einer gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten zuständigen nationalen Behörde als Mitglied des Verwaltungsrats. Erweist sich dies als nicht machbar, ernennt der Mitgliedstaat einen hochrangigen Vertreter einer gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten zuständigen nationalen Behörde als Mitglied des Verwaltungsrats.

(4) Die von der Kommission ernannten Mitglieder und die stellvertretenden Mitglieder des Verwaltungsrats werden aufgrund ihrer einschlägigen Kenntnisse im Bereich der Cybersicherheit sowie unter Berücksichtigung ihrer einschlägigen Leitungs-, Verwaltungs- und haushaltstechnischen Kompetenzen ernannt. Die Kommission und die Mitgliedstaaten streben in Bezug auf Stellvertreter eine ausgewogene Vertretung von Männern und Frauen im Verwaltungsrat an und bemühen sich, die Fluktuation gering zu halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen.

(5) Die Amtszeit der von den Mitgliedstaaten ernannten Mitglieder entspricht der Amtszeit ihrer in Absatz 3 genannten Funktion.

(6) Die Amtszeit der Stellvertreter und des von der Kommission ernannten Mitglieds beträgt vier Jahre. Sie kann verlängert werden.

Artikel 26
Vorsitz des Verwaltungsrats

(1) Der Verwaltungsrat wählt aus dem Kreis seiner stimmberechtigten Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden. Der Vorsitzende und der stellvertretende Vorsitzende werden mit Zweidrittelmehrheit der stimmberechtigten Mitglieder des Verwaltungsrats gewählt.

(2) Der stellvertretende Vorsitzende tritt im Falle der Verhinderung des Vorsitzenden automatisch an dessen Stelle.

(3) Die Amtszeit des Vorsitzenden und des stellvertretenden Vorsitzenden beträgt vier Jahre und kann einmal verlängert werden. Endet jedoch ihre Mitgliedschaft im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch am selben Tag.

Artikel 27
Sitzungen des Verwaltungsrats

(1) Der Vorsitzende beruft die Sitzungen des Verwaltungsrats ein.

(2) Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats teil, ist jedoch nicht stimmberechtigt.

(3) Der Verwaltungsrat tritt mindestens zweimal jährlich zu einer ordentlichen Sitzung zusammen. Zusätzlich tritt er auf Veranlassung seines Vorsitzenden, auf Antrag der Kommission oder auf Antrag von mindestens einem Drittel seiner Mitglieder zusammen.

(4) Ein Vertreter des mit der Verordnung (EU) 2021/887 eingerichteten Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit nimmt als ständiger Beobachter ohne Stimmrecht an den Sitzungen des Verwaltungsrats teil.

(5) Der Verwaltungsrat kann jede Person, deren Stellungnahme von Interesse sein könnte, als Ad-hoc-Beobachter ohne Stimmrecht und nach Maßgabe der Geschäftsordnung des Verwaltungsrats zu einer Sitzung oder einem Teil einer Sitzung einladen.

(6) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe der Geschäftsordnung des Verwaltungsrats von Beratern oder Sachverständigen bei den Sitzungen des Verwaltungsrats unterstützen lassen.

Artikel 28
Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat

a) legt die allgemeine Ausrichtung der Tätigkeit der ENISA fest und sorgt dafür, dass die ENISA ihre Geschäfte gemäß der in dieser Verordnung festgelegten Vorschriften und Grundsätze führt; er sorgt zudem für die Abstimmung der Arbeit der ENISA mit den Tätigkeiten, die von den Mitgliedstaaten und auf Unionsebene durchgeführt werden;

b) nimmt den Entwurf des in Artikel 44 genannten einheitlichen Programmplanungsdokuments der ENISA an, bevor dieser der Kommission zur Stellungnahme vorgelegt wird;

c) nimmt – unter Berücksichtigung der Stellungnahme der Kommission – im Einklang mit Artikel 29 Absatz 2 Buchstabe a das einheitliche Programmplanungsdokument der ENISA an;

d) beaufsichtigt die Umsetzung der im einheitlichen Programmplanungsdokument enthaltenen mehrjährigen und jährlichen Programmplanung;

e) nimmt im Einklang mit Artikel 29 Absatz 2 Buchstabe b den jährlichen Haushaltsplan der ENISA an und übt andere Funktionen in Bezug auf den Haushalt der ENISA gemäß Kapitel IV aus;

f) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der ENISA einschließlich des Jahresabschlusses und der Ausführungen darüber, inwiefern die ENISA die vorgegebenen Leistungsindikatoren erfüllt hat, und übermittelt den Bericht zusammen mit seiner Bewertung bis zum 1. Juli des folgenden Jahres dem Europäischen Parlament, dem Rat, der Kommission und dem Europäischen Rechnungshof, und macht ihn der Öffentlichkeit zugänglich;

g) erlässt nach Artikel 50 die für die ENISA geltende Finanzregelung;

h) nimmt eine Betrugsbekämpfungsstrategie an, die den diesbezüglichen Risiken entspricht und an einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen orientiert ist;

i) sorgt für geeignete Folgemaßnahmen zu den Feststellungen und Empfehlungen, die sich aus den internen oder externen Prüfberichten und Bewertungen sowie aus den Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (im Folgenden „OLAF“) und der Europäischen Staatsanwaltschaft (im Folgenden „EUStA“) ergeben;

j) gibt sich eine Geschäftsordnung einschließlich Regelungen zu den vorläufigen Beschlüssen zur Übertragung bestimmter Aufgaben gemäß Artikel 30 Absatz 7;

k) übt gemäß Absatz 2 gegenüber dem Personal der ENISA die Befugnisse aus, die der Anstellungsbehörde beziehungsweise der Einstellungsbehörde mit dem Statut der Beamten der Europäischen Union (im Folgenden „Statut“) und den Beschäftigungsbedingungen für die sonstigen Bediensteten der Union (im Folgenden „Beschäftigungsbedingungen“) – beide festgelegt durch die Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates[73] – übertragen wurden („Befugnisse der Anstellungsbehörde“);

l) erlässt gemäß Artikel 110 Absatz 2 des Statuts Durchführungsbestimmungen zu diesem Statut und den Beschäftigungsbedingungen;

m) ernennt im Einklang mit Artikel 31 den Exekutivdirektor und – sofern er die Schaffung des entsprechenden Postens beschließt – den stellvertretenden Exekutivdirektor und verlängert gegebenenfalls deren jeweilige Amtszeit oder beruft sie ab;

[73] ABl. L 56 vom 4.3.1968, S. 1, ELI: http://data.europa.eu/eli/reg/1968/259(1)/oj.

n) ernennt einen Rechnungsführer, der dem Statut und den Beschäftigungsbedingungen unterliegt und in der Wahrnehmung seiner Aufgaben unabhängig ist;

o) fasst unter Berücksichtigung der Tätigkeitserfordernisse der ENISA und unter Beachtung der Grundsätze einer wirtschaftlichen Haushaltsführung alle Beschlüsse über die Schaffung und, falls notwendig, Änderung der Organisationsstruktur der ENISA;

p) genehmigt den Abschluss von Arbeitsvereinbarungen bezüglich Artikel 68;

q) genehmigt den Abschluss von Arbeitsvereinbarungen gemäß Artikel 70;

r) ernennt die Mitglieder der Beschwerdekammer und beruft sie ab im Einklang mit Artikel 29 Absatz 2 Buchstabe d;

s) beschließt Vorschriften zur Verhinderung und Bewältigung von Interessenkonflikten der Mitglieder der Beschwerdekammer.

(2) Der Verwaltungsrat fasst gemäß Artikel 110 Absatz 2 des Statuts einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts und von Artikel 6 der Beschäftigungsbedingungen, mit dem er die einschlägigen Befugnisse der Anstellungsbehörde dem Exekutivdirektor überträgt und die Bedingungen festlegt, unter denen diese Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse einer nachgeordneten Ebene übertragen.

(3) Wenn außergewöhnliche Umstände dies erfordern, kann der Verwaltungsrat durch Beschluss die Übertragung der Befugnisse der Anstellungsbehörde auf den Exekutivdirektor sowie jegliche von diesem vorgenommene Weiterübertragung von Befugnissen der Anstellungsbehörde vorübergehend aussetzen und die Befugnisse selbst ausüben oder sie stattdessen einem seiner Mitglieder oder einem anderen Bediensteten als dem Exekutivdirektor übertragen.

Artikel 29
Vorschriften für die Abstimmung im Verwaltungsrat

(1) Sofern in dieser Verordnung nichts anderes bestimmt ist, fasst der Verwaltungsrat seine Beschlüsse mit der absoluten Mehrheit seiner stimmberechtigten Mitglieder.

(2) Eine Zweidrittelmehrheit der stimmberechtigten Mitglieder des Verwaltungsrats ist erforderlich für

a) die Annahme des in Artikel 28 Absatz 1 Buchstabe c genannten einheitlichen Programmplanungsdokuments;

b) die Annahme des in Artikel 28 Absatz 1 Buchstabe e genannten jährlichen Haushaltsplans;

c) die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors und des stellvertretenden Exekutivdirektors gemäß den Artikeln 31 und 33;

d) die Ernennung und Abberufung der Mitglieder der in Artikel 36 genannten Beschwerdekammer.

(3) Beschlüsse in Haushalts- und Personalangelegenheiten, insbesondere in Bezug auf die in Artikel 28 Absatz 1 Buchstaben c, e, f, g, h, i, k, l, m und n genannte Angelegenheiten können nur gefasst werden, wenn auch die Vertreter der

Kommission dafür stimmen. Die Annahme der in Artikel 28 Absatz 1 Buchstabe c genannten Beschlüsse über das einheitliche Programmplanungsdokument der ENISA bedarf nur für die Elemente des Beschlusses, die nicht mit dem jährlichen und mehrjährigen Arbeitsprogramm der ENISA im Zusammenhang stehen, eines zustimmenden Votums des Vertreters der Kommission.

(4) Jedes stimmberechtigte Mitglied hat eine Stimme. Bei Abwesenheit eines stimmberechtigten Mitglieds ist sein Stellvertreter berechtigt, das Stimmrecht des Mitglieds auszuüben.

(5) Der Vorsitzende des Verwaltungsrats nimmt an den Abstimmungen teil.

(6) Der Exekutivdirektor nimmt nicht an den Abstimmungen teil.

(7) Die näheren Einzelheiten der Abstimmungsregeln, insbesondere die Voraussetzungen, unter denen ein Mitglied im Namen eines anderen Mitglieds handeln kann, werden in der Geschäftsordnung des Verwaltungsrats festgelegt.

Abschnitt 2
Exekutivrat

Artikel 30
Exekutivrat

(1) Der Verwaltungsrat wird von einem Exekutivrat unterstützt.

(2) Der Exekutivrat

a) bereitet die Beschlussvorlagen für den Verwaltungsrat vor;

b) sorgt gemeinsam mit dem Verwaltungsrat für angemessene Folgemaßnahmen zu den Feststellungen und Empfehlungen, die sich aus den internen oder externen Prüfberichten und Bewertungen sowie den Untersuchungen des OLAF und der EUStA ergeben;

c) unterstützt und berät den in Artikel 32 genannten Exekutivdirektor unbeschadet dessen Zuständigkeiten in Bezug auf die Umsetzung der Beschlüsse des Verwaltungsrats im Hinblick auf eine verstärkte Aufsicht über die Verwaltung und Haushaltsführung.

(3) Der Exekutivrat setzt sich aus dem Vorsitzenden des Verwaltungsrats, einem Vertreter der Kommission im Verwaltungsrat und drei anderen stimmberechtigten Mitgliedern zusammen, die der Verwaltungsrat aus den eigenen Reihen bestimmt. Der Vorsitzende des Verwaltungsrats führt auch den Vorsitz im Exekutivrat. Bei den Ernennungen der Mitglieder des Exekutivrats wird ein ausgewogenen Geschlechterverhältnis im Exekutivrat angestrebt. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats teil, hat jedoch kein Stimmrecht.

(4) Die Amtszeit der Mitglieder des Exekutivrats beträgt vier Jahre. Sie kann verlängert werden. Die Amtszeit der Mitglieder des Exekutivrats endet mit dem Ende ihrer Mitgliedschaft im Verwaltungsrat.

(5) Der Exekutivrat hält mindestens alle drei Monate eine ordentliche Sitzung ab. Zusätzlich tritt er auf Veranlassung seines Vorsitzenden oder auf Antrag seiner Mitglieder zusammen.

(6) Der Verwaltungsrat legt die Geschäftsordnung des Exekutivrats fest.

(7) Ist dies aufgrund der Dringlichkeit notwendig, so kann der Exekutivrat im Namen des Verwaltungsrats bestimmte vorläufige Beschlüsse fassen, vor allem in Verwaltungsangelegenheiten, einschließlich der Aussetzung der Übertragung der Befugnisse der Anstellungsbehörde, und in Haushaltsangelegenheiten. Diese vorläufigen Beschlüsse werden dem Verwaltungsrat unverzüglich mitgeteilt. Der Verwaltungsrat entscheidet sodann spätestens drei Monate, nachdem der Beschluss gefasst wurde, ob er den vorläufigen Beschluss genehmigt oder ob er ihn nicht genehmigt. Der Exekutivrat fasst keine Beschlüsse im Namen des Verwaltungsrats, die mit einer Zweidrittelmehrheit der stimmberechtigten Mitglieder des Verwaltungsrats angenommen werden müssen.

Abschnitt 3
Exekutivdirektor

Artikel 31
Ernennung und Abberufung sowie Verlängerung der Amtszeit

(1) Der Exekutivdirektor wird vom Verwaltungsrat auf der Grundlage seiner Verdienste und Kompetenzen aus einer Liste von Kandidaten ernannt, die von der Kommission nach einem offenen und transparenten Auswahlverfahren vorgeschlagen werden.

(2) Vor der Ernennung wird der vom Verwaltungsrat ausgewählte Kandidat aufgefordert, eine Erklärung vor dem zuständigen Ausschuss des Europäischen Parlaments abzugeben und Fragen der Mitglieder zu beantworten.

(3) Der Exekutivdirektor wird als Zeitbediensteter der ENISA gemäß Artikel 2 Buchstabe a der Beschäftigungsbedingungen eingestellt.

(4) Für den Abschluss des Vertrages mit dem Exekutivdirektor wird die ENISA durch den Vorsitzenden des Verwaltungsrats vertreten.

(5) Die Amtszeit des Exekutivdirektors beträgt fünf Jahre. Rechtzeitig vor Ende dieses Zeitraums nimmt die Kommission eine Bewertung vor, die der Leistung des Exekutivdirektors und den künftigen Aufgaben und Herausforderungen der ENISA Rechnung trägt.

(6) Der Verwaltungsrat kann die Amtszeit des Exekutivdirektors auf Vorschlag der Kommission, die der Bewertung nach Absatz 5 Rechnung trägt, einmal um höchstens fünf Jahre verlängern.

(7) Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, darf am Ende seiner gesamten Amtszeit nicht an einem anderen Auswahlverfahren für dieselbe Stelle teilnehmen.

(8) Der Verwaltungsrat unterrichtet das Europäische Parlament über seine Absicht, die Amtszeit des Exekutivdirektors gemäß Absatz 6 zu verlängern. Innerhalb von drei Monaten vor der Verlängerung der Amtszeit gibt der Exekutivdirektor, sofern er dazu aufgefordert wird, vor dem zuständigen Ausschuss des Europäischen Parlaments eine Erklärung ab und beantwortet Fragen der Mitglieder.

(9) Der Exekutivdirektor kann nur mit Beschluss des Verwaltungsrats auf Vorschlag der Kommission abberufen werden.

Artikel 32
Aufgaben und Zuständigkeiten des Exekutivdirektors

(1) Der Exekutivdirektor leitet die ENISA und ist dem Verwaltungsrat gegenüber rechenschaftspflichtig.

(2) Der Exekutivdirektor übt sein Amt unabhängig aus und darf Weisungen von Regierungen oder sonstigen Stellen weder einholen und entgegennehmen.

(3) Der Exekutivdirektor erstattet dem Europäischen Parlament über die Wahrnehmung seiner Aufgaben Bericht, wenn er dazu aufgefordert wird. Der Rat kann den Exekutivdirektor auffordern, über die Wahrnehmung seiner Aufgaben Bericht zu erstatten.

(4) Der Exekutivdirektor ist der gesetzliche Vertreter der ENISA.

(5) Der Exekutivdirektor ist für die Erfüllung der Aufgaben zuständig, die der ENISA durch diese Verordnung zugewiesenen werden. Der Exekutivdirektor ist insbesondere dafür zuständig,

a) die Führung der laufenden Geschäfte der ENISA zu gewährleisten;

b) die Beschlüsse des Verwaltungsrats durchzuführen;

c) die Einhaltung der für die ENISA geltenden Finanzregelung zu gewährleisten;

d) den Entwurf des einheitlichen Programmplanungsdokuments auszuarbeiten und dem Verwaltungsrat vor der Übermittlung an die Kommission zur Stellungnahme vorzulegen;

e) das einheitliche Programmplanungsdokument umzusetzen und dem Verwaltungsrat über seine Umsetzung Bericht zu erstatten;

f) den konsolidierten jährlichen Tätigkeitsbericht der ENISA, einschließlich der Umsetzung des Jahresarbeitsprogramms der ENISA, auszuarbeiten und dem Verwaltungsrat zur Bewertung und Annahme vorzulegen;

g) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen der nachträglichen Bewertungen der ENISA gemäß Artikel 121 auszuarbeiten und alle zwei Jahre der Kommission über die erzielten Fortschritte Bericht zu erstatten;

h) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte und der Bewertungen sowie der Untersuchungen des OLAF und der EUStA auszuarbeiten und der Kommission zweimal jährlich sowie dem Verwaltungsrat regelmäßig über die erzielten Fortschritte Bericht zu erstatten;

i) den Entwurf der für die ENISA geltenden Finanzregelung nach Artikel 50 auszuarbeiten;

j) den Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA auszuarbeiten und ihren Haushaltsplan auszuführen;

k) die finanziellen Interessen der Union durch vorbeugende Maßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen – unbeschadet der Untersuchungsbefugnisse des OLAF und der EUStA – und, falls Unregelmäßigkeiten festgestellt werden, durch Einziehung rechtsgrundlos gezahlter Beträge sowie gegebenenfalls durch wirksame,

verhältnismäßige und abschreckende verwaltungsrechtliche und finanzielle Sanktionen zu schützen;

l) eine Betrugsbekämpfungsstrategie, eine Strategie für Effizienzgewinne und Synergien, eine Strategie für die Zusammenarbeit mit Drittländern oder internationalen Organisationen sowie eine Strategie für die Systeme des Organisationsmanagements und der internen Kontrolle für die ENISA auszuarbeiten und dem Verwaltungsrat zur Genehmigung vorzulegen;

m) Kontakte zur Wirtschaft und zu Verbraucherorganisationen im Hinblick auf einen regelmäßigen Dialog mit den einschlägigen Interessenträgern aufzubauen und zu pflegen;

n) einen regelmäßigen Gedanken- und Informationsaustausch mit den einschlägigen Einrichtungen der Union über deren Tätigkeiten im Bereich Cybersicherheit zu führen, um die Kohärenz bei der Umsetzung der diesbezüglichen Unionspolitik sicherzustellen;

o) die Vielfalt und ein ausgewogenes Geschlechterverhältnisses bei der Einstellung des Personals der ENISA zu fördern;

p) Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Artikel 20 Absatz 1 anzunehmen;

q) Entscheidungen in Bezug auf Antragsteller gemäß Artikel 22 Absatz 3 zu treffen, die befugte Bescheinigungsanbieter werden oder ihre Befugnis verlängern lassen wollen;

r) sonstige dem Exekutivdirektor durch diese Verordnung übertragene Aufgaben wahrzunehmen.

(6) Soweit erforderlich sowie entsprechend den Zielen und Aufgaben der ENISA kann der Exekutivdirektor der ENISA Ad-hoc-Arbeitsgruppen aus Sachverständigen – auch von den zuständigen Behörden der Mitgliedstaaten – einsetzen. Der Exekutivdirektor unterrichtet den Verwaltungsrat hiervon vorab. Die Verfahren, die insbesondere die Zusammensetzung dieser Arbeitsgruppen, die Bestellung der Sachverständigen der Arbeitsgruppen durch den Exekutivdirektor und die Arbeitsweise der Arbeitsgruppen betreffen, werden in den internen Verfahrensvorschriften der ENISA festgelegt.

(7) Der Exekutivdirektor kann auf der Grundlage einer angemessenen Kosten-Nutzen-Analyse erforderlichenfalls beschließen, eine oder mehrere Außenstellen in einem oder mehreren Mitgliedstaaten einzurichten, damit die ENISA ihre Aufgaben effizient und wirksam wahrnehmen kann. Bevor er über die Einrichtung einer Außenstelle beschließt, ersucht der Exekutivdirektor den/die betreffenden Mitgliedstaat(en), einschließlich des Mitgliedstaats, in dem die ENISA ihren Sitz hat, um eine Stellungnahme, und er holt die vorherige Zustimmung der Kommission und des Verwaltungsrats ein. Im Falle von Meinungsverschiedenheiten bei der Konsultation zwischen dem Exekutivdirektor und den betreffenden Mitgliedstaaten werden die strittigen Fragen dem Rat zur Erörterung vorgelegt. Die Gesamtzahl der Mitarbeiter in allen Außenstellen ist möglichst gering zu halten und darf insgesamt nicht 40 % der Gesamtzahl der Mitarbeiter der ENISA in dem Mitgliedstaat, in dem die ENISA ihren Sitz hat, überschreiten. Die Anzahl der Mitarbeiter in jeder Außenstelle darf nicht 10 % der Gesamtzahl der Mitarbeiter der Agentur im Mitgliedstaat, in dem die ENISA ihren Sitz hat, überschreiten.

(8) In dem Beschluss zur Einrichtung einer Außenstelle wird der Umfang der in der Außenstelle auszuübenden Tätigkeiten so festgelegt, dass unnötige Kosten und eine Überschneidung der Verwaltungsfunktionen mit denen der ENISA vermieden werden.

Abschnitt 4
Stellvertretender Exekutivdirektor

Artikel 33
Stellvertretender Exekutivdirektor

(1) Der Verwaltungsrat kann beschließen, einen stellvertretenden Exekutivdirektor einzusetzen, der den Exekutivdirektor unterstützt.

(2) Beschließt der Verwaltungsrat die Schaffung des Postens eines stellvertretenden Exekutivdirektors, gelten die Bestimmungen des Artikel 31 entsprechend für diesen.

Artikel 34
Aufgaben und Zuständigkeiten des stellvertretenden Exekutivdirektors

Der stellvertretende Exekutivdirektor unterstützt den Exekutivdirektor bei der Leitung der ENISA und der Wahrnehmung der in Artikel 32 genannten Aufgaben. Bei Abwesenheit oder Verhinderung des Exekutivdirektors oder sofern der Posten unbesetzt ist, tritt der stellvertretende Exekutivdirektor für die Zeit der Abwesenheit oder bis zur Besetzung des Postens an seine Stelle.

Abschnitt 5
ENISA-Beratungsgruppe

Artikel 35
ENISA-Beratungsgruppe

(1) Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors auf transparente Art und Weise die ENISA-Beratungsgruppe ein. Die ENISA-Beratungsgruppe setzt sich aus anerkannten Sachverständigen zusammen, die einschlägige Interessenträger vertreten, darunter die Cybersicherheitsbranche, die IKT-Branche, KMU, Einrichtungen, die in den in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren tätig sind, Hersteller von Produkten mit digitalen Elementen und Verwalter quelloffener Software im Sinne der Verordnung (EU) 2024/2847, Konformitätsbewertungsstellen, die nach dem europäischen Rahmen für die Cybersicherheitszertifizierung gemäß Artikel 93 und der Verordnung (EU) 2024/2847 notifiziert wurden, Einrichtungen, die im Bereich der elektronischen Identifizierungsmittel tätig sind, Verbrauchergruppen, wissenschaftliche Sachverständige aus dem Bereich der Cybersicherheit, europäische Normungsorganisationen sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden. Diese anerkannten Sachverständigen müssen Staatsangehörige von Mitgliedstaaten sein. Der Verwaltungsrat strebt ein angemessenes Gleichgewicht zwischen den Geschlechtern, ein angemessenes geografisches Gleichgewicht und ein angemessenes Gleichgewicht zwischen den verschiedenen Interessengruppen an.

(2) Die Verfahren für die ENISA-Beratungsgruppe, insbesondere in Bezug auf ihre Zusammensetzung, den in Absatz 1 genannten Vorschlag des Exekutivdirektors, die Anzahl und die Ernennung der Mitglieder und die Arbeitsweise der ENISA-Beratungsgruppe, werden in den internen Verfahrensvorschriften der ENISA festgelegt und öffentlich bekannt gemacht.

(3) Den Vorsitz der ENISA-Beratungsgruppe führt der Exekutivdirektor oder eine jeweils vom Exekutivdirektor ernannte Person.

(4) Die Amtszeit der Mitglieder der ENISA-Beratungsgruppe beträgt zweieinhalb Jahre und kann einmal verlängert werden. Mitglieder des Verwaltungsrats dürfen nicht Mitglieder der ENISA-Beratungsgruppe sein. Sachverständige der Kommission und Sachverständige aus den Mitgliedstaaten können an den Sitzungen der ENISA-Beratungsgruppe teilnehmen und an ihrer Arbeit mitwirken. Der Exekutivdirektor kann Vertreter anderer Stellen, die der ENISA-Beratungsgruppe nicht angehören, zur Teilnahme an den Sitzungen der ENISA-Beratungsgruppe und zur Mitwirkung an ihrer Arbeit eingeladen.

(5) Die ENISA-Beratungsgruppe berät die ENISA bei der Durchführung ihrer Aufgaben, ausgenommen der Anwendung der Bestimmungen der Titel III, IV und V dieser Verordnung. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Jahresarbeitsprogramms der ENISA und bei der Kommunikation mit den einschlägigen Interessenträgern in Bezug auf Fragen im Zusammenhang mit dem Jahresarbeitsprogramm.

(6) Die ENISA-Beratungsgruppe unterrichtet den Verwaltungsrat regelmäßig über ihre Tätigkeiten.

(7) Die ENISA leistet die logistische Unterstützung, die für die Arbeit der ENISA-Beratungsgruppe erforderlich ist, und stellt ein Sekretariat für deren Sitzungen.

Abschnitt 6
Beschwerdekammer

Artikel 36
Einrichtung und Zusammensetzung der Beschwerdekammer

(1) Die ENISA richtet eine Beschwerdekammer durch einen Beschluss des Verwaltungsrats ein.

(2) Die Beschwerdekammer besteht aus einem Vorsitzenden und drei weiteren Mitgliedern. Jedes Mitglied der Beschwerdekammer hat einen Stellvertreter. Der Stellvertreter vertritt das Mitglied in dessen Abwesenheit.

(3) Der Vorsitzende, die weiteren Mitglieder und ihre Stellvertreter werden vom Verwaltungsrat anhand einer von der Kommission festgelegten Liste qualifizierter Kandidaten ernannt. Die Liste der qualifizierten Kandidaten gilt vier Jahre lang. Die Gültigkeit der Liste kann auf Vorschlag der Kommission vom Verwaltungsrat um jeweils vier Jahre verlängert werden.

(4) Die Beschwerdekammer kann den Verwaltungsrat ersuchen, zwei zusätzliche Mitglieder und deren Stellvertreter von der in Absatz 3 genannten Liste zu ernennen, wenn sie der Ansicht ist, dass die Art der Beschwerde dies erfordert.

(5) Die Beschwerdekammer gibt sich eine Geschäftsordnung und veröffentlicht diese.

Artikel 37
Mitglieder der Beschwerdekammer

(1) Die Amtszeit der Mitglieder der Beschwerdekammer und ihrer Stellvertreter beträgt vier Jahre. Ihre Amtszeit kann auf Vorschlag der Kommission vom Verwaltungsrat um jeweils vier Jahre verlängert werden.

(2) Die Mitglieder der Beschwerdekammer sind unabhängig und nehmen keine anderen Aufgaben innerhalb der ENISA wahr. Bei ihren Entscheidungen dürfen sie Weisungen von Regierungen, sonstigen Stellen oder privaten Einrichtungen weder einholen noch entgegennehmen.

(3) Die Mitglieder der Beschwerdekammer dürfen während ihrer jeweiligen Amtszeit nur aus schwerwiegenden Gründen auf Vorschlag der Kommission vom Verwaltungsrat mit einem entsprechenden Beschluss abberufen oder von der Liste qualifizierter Kandidaten gestrichen werden.

Artikel 38
Ausschluss und Ablehnung

(1) Die Mitglieder der Beschwerdekammer dürfen nicht an einem Beschwerdeverfahren mitwirken, wenn dieses Verfahren ihre persönlichen Interessen berührt, wenn sie zuvor als Vertreter eines Verfahrensbeteiligten tätig gewesen sind oder wenn sie an dem Beschluss mitgewirkt haben, der Gegenstand der Beschwerde ist.

(2) Ist ein Mitglied einer Beschwerdekammer aus einem der in Absatz 1 aufgeführten Gründe oder aus einem sonstigen Grund der Ansicht, an einem Beschwerdeverfahren nicht mitwirken zu können, so teilt es dies der Beschwerdekammer mit.

(3) Ein am Beschwerdeverfahren Beteiligter kann ein Mitglied einer Beschwerdekammer aus einem der in Absatz 1 aufgeführten Gründe oder wegen des Verdachts der Befangenheit ablehnen. Die Ablehnung ist nicht zulässig, wenn der am Beschwerdeverfahren Beteiligte Verfahrenshandlungen vorgenommen hat, obwohl er den Ablehnungsgrund kannte. Die Ablehnung darf nicht mit der Staatsangehörigkeit der Mitglieder der Beschwerdekammer begründet werden.

(4) Die Beschwerdekammer entscheidet über das Vorgehen in den Fällen der Absätze 2 und 3 ohne Mitwirkung des betreffenden Mitglieds. Das betreffende Mitglied wird bei diesem Beschluss durch seinen Stellvertreter in der Beschwerdekammer vertreten.

Artikel 39
Beschwerden gegen Entscheidungen und wegen Untätigkeit

(1) Die Beschwerdekammer kann mit Beschwerden gegen Folgendes befasst werden:

a) Entscheidungen der ENISA gemäß Artikel 22 Absatz 3;

b) Versäumnis der ENISA, innerhalb der in Artikel 22 Absatz 4 festgelegten geltenden Fristen tätig zu werden.

(2) Eine gemäß Absatz 1 eingelegte Beschwerde unterliegt einem Abhilfeverfahren gemäß Artikel 41, bevor sie der Beschwerdekammer zur Prüfung vorgelegt wird.

(3) Eine Beschwerde nach Absatz 1 hat keine aufschiebende Wirkung.

Artikel 40
Beschwerdeberechtigte, Frist und Form

(1) Antragsteller im Sinne des Artikels 21 Absatz 3 können Rechtsmittel einlegen gegen

a) eine an sie gerichtete Entscheidung der ENISA gemäß Artikel 22 Absatz 3;

b) ein Versäumnis der ENISA, innerhalb der in Artikel 22 Absatz 4 festgelegten geltenden Fristen in Bezug auf den von ihnen eingereichten Antrag tätig zu werden.

(2) In dem in Absatz 1 Buchstabe a genannten Fall ist die Beschwerde zusammen mit einer Begründung gemäß Artikel 36 Absatz 5 innerhalb von zwei Monaten nach Bekanntgabe der Entscheidung an den betreffenden Beschwerdeführer oder, falls keine Bekanntgabe erfolgt ist, innerhalb von zwei Monaten ab dem Zeitpunkt, zu dem der Beschwerdeführer von der Entscheidung Kenntnis erlangt hat, schriftlich einzulegen.

(3) In dem in Absatz 1 Buchstabe b genannten Fall ist die Beschwerde gemäß der in Artikel 36 Absatz 5 genannten Geschäftsordnung innerhalb von zwei Monaten nach Ablauf der in Artikel 22 Absatz 4 genannten Frist schriftlich bei der ENISA einzulegen.

Artikel 41
Abhilfe

(1) Erachtet die ENISA die Beschwerde als zulässig und begründet, so korrigiert sie die Entscheidung oder die Untätigkeit gemäß Artikel 40 Absatz 1.

(2) Wird die Entscheidung nicht innerhalb eines Monats nach Eingang der Beschwerde von der ENISA korrigiert, so entscheidet die ENISA umgehend, ob sie den Vollzug ihrer Entscheidung aussetzt, und legt die Beschwerde der Beschwerdekammer vor.

Artikel 42
Prüfung der Entscheidung über Beschwerden

(1) Die Beschwerdekammer entscheidet innerhalb von drei Monaten nach Einreichung einer Beschwerde, ob sie dieser stattgibt oder sie zurückweist. Bei der Prüfung einer Beschwerde wird die Beschwerdekammer innerhalb der in ihrer Geschäftsordnung festgelegten Fristen tätig. Sie fordert die am Beschwerdeverfahren Beteiligten so oft wie erforderlich auf, innerhalb bestimmter Fristen Stellungnahmen zu ihren Bescheiden oder zu den Schriftsätzen der anderen Beteiligten des Beschwerdeverfahrens einzureichen. Die am Beschwerdeverfahren Beteiligten haben das Recht, mündliche Erklärungen abzugeben.

(2) Stellt die Beschwerdekammer fest, dass die Beschwerde begründet ist, verweist sie die Angelegenheit an die ENISA zurück. Die ENISA trifft ihre endgültige Entscheidung in Übereinstimmung mit den Feststellungen der Beschwerdekammer und begründet diese Entscheidung. Die ENISA unterrichtet die Beteiligten des Beschwerdeverfahrens hierüber.

Artikel 43
Klagen beim Gerichtshof der Europäischen Union

(1) Klagen zur Aufhebung von Entscheidungen der ENISA, die gemäß Artikel 22 Absatz 3 getroffen wurden, oder Klagen wegen Untätigkeit gemäß Artikel 22 Absatz 4 können beim Gerichtshof der Europäischen Union erhoben werden, nachdem das in den Artikeln 39 bis 42 vorgesehene Beschwerdeverfahren innerhalb der ENISA ausgeschöpft wurde, oder bei Untätigkeit innerhalb der geltenden Frist gemäß Artikel 41 Absatz 2.

(2) Die ENISA hat alle erforderlichen Maßnahmen zu ergreifen, um dem Urteil des Gerichtshofs der Europäischen Union nachzukommen.

Abschnitt 7
Betriebstätigkeiten

Artikel 44
Einheitliches Programmplanungsdokument

(1) Die ENISA führt ihre Geschäfte in Übereinstimmung mit einem einheitlichen Programmplanungsdokument, das ihr jährliches und mehrjähriges Arbeitsprogramm mit allen ihren geplanten Tätigkeiten enthält.

(2) Jedes Jahr erstellt der Exekutivdirektor einen Entwurf des in Absatz 1 genannten einheitlichen Programmplanungsdokuments und der entsprechenden Finanz- und Personalplanung nach Artikel 32 der Delegierten Verordnung (EU) 2019/715 der Kommission[74] und unter Berücksichtigung der von der Kommission festgelegten Leitlinien.

(3) Bis zum 30. November eines jeden Jahres nimmt der Verwaltungsrat das in Absatz 1 genannte einheitliche Programmplanungsdokument an, wobei er die Stellungnahme der Kommission nach Artikel 32 Absatz 7 der Delegierten Verordnung (EU) 2019/715 der Kommission berücksichtigt. Wenn der Verwaltungsrat beschließt, Teile der Stellungnahme der Kommission nicht zu berücksichtigen, legt er eine ausführliche Begründung für diesen Beschluss vor. Der Verwaltungsrat leitet das einheitliche Programmplanungsdokument bis zum 31. Januar des Folgejahres sowie jede spätere Aktualisierung dieses Dokuments an das Europäische Parlament, den Rat und die Kommission weiter.

(4) Das einheitliche Programmplanungsdokument wird nach der endgültigen Feststellung des Gesamthaushaltsplans der Union endgültig und ist erforderlichenfalls entsprechend anzupassen.

(5) Das Jahresarbeitsprogramm enthält detaillierte Ziele und Angaben zu den erwarteten Ergebnissen, einschließlich Erfolgsindikatoren. Es enthält zudem eine Beschreibung der zu finanzierenden Maßnahmen sowie Angaben zur Höhe der für die einzelnen Maßnahmen vorgesehenen finanziellen und personellen Ressourcen gemäß den Grundsätzen der maßnahmenbezogenen Aufstellung des Haushaltsplans und des

[74] Delegierte Verordnung (EU) 2019/715 der Kommission vom 18. Dezember 2018 über die Rahmenfinanzregelung für gemäß dem AEUV und dem Euratom-Vertrag geschaffene Einrichtungen nach Artikel 70 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates (ABl. L 122 vom 10.5.2019, S. 1, ELI: http://data.europa.eu/eli/reg_del/2019/715/oj).

maßnahmenbezogenen Managements. Das Jahresarbeitsprogramm muss mit dem mehrjährigen Arbeitsprogramm nach Absatz 7 im Einklang stehen. Es ist klar darin anzugeben, welche Aufgaben im Vergleich zum vorangegangenen Haushaltsjahr hinzugefügt, verändert oder gestrichen wurden.

(6) Der Verwaltungsrat ändert das angenommene Jahresarbeitsprogramm, wenn der ENISA eine neue Aufgabe zugewiesen wird. Wesentliche Änderungen des Jahresarbeitsprogramms werden nach demselben Verfahren angenommen wie das ursprüngliche Jahresarbeitsprogramm. Der Verwaltungsrat kann dem Exekutivdirektor die Befugnis übertragen, nicht wesentliche Änderungen am Jahresarbeitsprogramm vorzunehmen.

(7) Im mehrjährigen Arbeitsprogramm der Agentur wird die strategische Gesamtplanung einschließlich der Ziele, erwarteten Ergebnisse und Leistungsindikatoren festgelegt. Es umfasst auch die Ressourcenplanung mit einem mehrjährigen Finanz- und Personalplan.

(8) Die Ressourcenplanung wird jährlich aktualisiert. Die strategische Programmplanung ist zu aktualisieren, wann immer dies geboten erscheint und insbesondere, wenn dies notwendig ist, um dem Ergebnis der in Artikel 120 genannten Bewertung Rechnung zu tragen.

KAPITEL IV
Aufstellung und Gliederung des Haushaltsplans der ENISA

Artikel 45
Aufstellung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor erstellt jedes Jahr einen vorläufigen Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr, einschließlich des Stellenplans, und übermittelt ihn dem Verwaltungsrat.

(2) Der vorläufige Entwurf des Voranschlags basiert auf den im Jahresarbeitsprogramm niedergelegten Zielen und erwarteten Ergebnissen und trägt den finanziellen Ressourcen, die für die Verwirklichung dieser Ziele und erwarteten Ergebnisse benötigt werden, Rechnung, wobei der Grundsatz der Wirtschaftlichkeit der Haushaltsführung und der Leistungsorientierung zu beachten ist.

(3) Auf der Grundlage des vorläufigen Entwurfs des Voranschlags verabschiedet der Verwaltungsrat einen Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr und übermittelt ihn jedes Jahr bis zum 31. Januar der Kommission.

(4) Die Kommission übermittelt den Entwurf des Voranschlags zusammen mit dem Entwurf des Gesamthaushaltsplans der Union der Haushaltsbehörde. Der Entwurf des Voranschlags wird auch der ENISA zur Verfügung gestellt.

(5) Auf der Grundlage des Entwurfs des Voranschlags setzt die Kommission die von ihr als erforderlich erachteten Mittelansätze für den Stellenplan und den Betrag des Beitrags aus dem Gesamthaushaltsplan in den Entwurf des Gesamthaushaltsplans der Union ein, den sie gemäß den Artikeln 313 und 314 AEUV der Haushaltsbehörde vorlegt.

(6) Die Haushaltsbehörde bewilligt die Mittel für den aus dem Gesamthaushaltsplan der Union finanzierten Beitrag zur ENISA.

(7) Die Haushaltsbehörde genehmigt den Stellenplan der ENISA.

(8) Der Verwaltungsrat stellt den Haushaltsplan der ENISA fest. Er wird endgültig, wenn der Gesamthaushaltsplan der Union endgültig festgestellt ist, und ist erforderlichenfalls entsprechend anzupassen.

(9) Für Immobilienprojekte, die voraussichtlich erhebliche Auswirkungen auf den Haushalt der ENISA haben, gilt die Delegierte Verordnung (EU) 2019/715.

Artikel 46
Gliederung des Haushaltsplans der ENISA

(1) Für jedes Haushaltsjahr wird ein Voranschlag sämtlicher Einnahmen und Ausgaben der ENISA erstellt und im Haushaltsplan der ENISA ausgewiesen. Das Haushaltsjahr entspricht dem Kalenderjahr.

(2) Der Haushalt der ENISA muss in Bezug auf Einnahmen und Ausgaben ausgeglichen sein.

(3) Unbeschadet sonstiger Ressourcen gliedern sich die Einnahmen der ENISA wie folgt:

a) ein Beitrag der Union aus dem Gesamthaushaltsplan der Union;

b) Einnahmen, die konkreten Ausgabenpositionen im Einklang mit der in Artikel 50 genannten Finanzregelung zugewiesen werden;

c) Unionsmittel in Form von Beitragsvereinbarungen oder Ad-hoc-Finanzhilfen im Einklang mit der in Artikel 50 genannten Finanzregelung der ENISA und den Bestimmungen der einschlägigen Instrumente zur Unterstützung der Unionspolitik;

d) die Gebühren, die zulasten der Antragsteller für Tätigkeiten im Zusammenhang mit Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Artikel 22 Absatz 1 erhoben werden;

e) die Gebühren, die zulasten der Konformitätsbewertungsstellen für die Teilnahme an europäischen Cybersicherheitszertifikaten und die Ausstellung von Zertifikaten im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung gemäß Artikel 47 Absatz 2 erhoben werden;

f) die Gebühren, die zulasten von Behörden oder privaten Stellen für in Artikel 47 Absatz 3 genannte Testinstrumente erhoben werden;

g) Beiträge von Drittländern, die sich nach Artikel 70 Absatz 4 an der Arbeit der ENISA beteiligen,

h) freiwillige Zahlungen oder Sachleistungen von Mitgliedstaaten.

(4) Mitgliedstaaten, die einen freiwilligen Beitrag nach Absatz 3 Buchstabe g leisten, können aufgrund dessen keine bestimmten Rechte oder Dienstleistungen beanspruchen.

(5) Die Ausgaben der ENISA umfassen die Bezüge des Personals, die Verwaltungs- und Infrastrukturausgaben sowie die operativen Ausgaben.

Artikel 47
Gebühren

(1) Für jede Tätigkeit im Rahmen des Systems europäischer Bescheinigungen gemäß Artikel 22 Absatz 1 werden zulasten von Antragstellern im Sinne des Artikels 21 Absatz 3 oder von befugten Bescheinigungsanbietern als Beitrag zur vollständigen Deckung der Kosten der von der ENISA durchgeführten Tätigkeiten folgende Gebühren erhoben:

a) Erteilung von Befugnissen nach Prüfung der in Artikel 21 Absätze 3 und 4 festgelegten Anforderungen, einschließlich der Durchführung von Bewertungen;

b) jährliche Aufrechterhaltung der Befugnis;

c) Verlängerung der Befugnisse für Anbieter europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, einschließlich der Durchführung von Bewertungen.

(2) Im Zusammenhang mit der Zertifizierung werden für die Pflege der europäischen Systeme für die Cybersicherheitszertifizierung, in deren Rahmen europäische Cybersicherheitszertifikate ausgestellt werden, zulasten der Konformitätsbewertungsstellen insbesondere folgende Gebühren erhoben:

a) eine jährliche Gebühr für die Teilnahme an einem europäischen System für die Cybersicherheitszertifizierung;

b) eine Gebühr für die Ausstellung europäischer Cybersicherheitszertifikate im Rahmen europäischer Systeme für die Cybersicherheitszertifizierung.

Die unter Buchstabe b genannten Gebühren werden erhoben, wenn die Konformitätsbewertungsstelle der ENISA europäische Cybersicherheitszertifikate zur Veröffentlichung auf ihrer Website gemäß Artikel 79 übermittelt.

(3) In Bezug auf die in Artikel 15 Absatz 1 genannten Testinstrumente wird für deren Nutzung eine Gebühr zulasten der Behörde oder privaten Stelle erhoben.

(4) Gebühren werden in Euro angegeben und entrichtet.

(5) Die Kommission erlässt Durchführungsrechtsakte mit Durchführungsbestimmungen für die Festsetzung der von der ENISA zu erhebenden Gebühren, in denen insbesondere die geschätzten Kosten für jede der Angelegenheiten, für die Gebühren gemäß den Absätzen 1, 2 und 3 zu entrichten sind, und die einzelnen zu entrichtenden Gebührenbeträge sowie die Modalitäten und Bedingungen, unter denen die Gebühren zu entrichten sind, präzisiert werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen. Bei der Ausarbeitung der Entwürfe dieser Durchführungsrechtsakte konsultiert die Kommission die ENISA.

(6) Die in den in Absatz 5 genannten Durchführungsrechtsakten festgelegten Gebühren werden im Voraus so festgelegt, dass sie in einem angemessenen Verhältnis zu den ermittelten geschätzten Kosten der auf kosteneffiziente Weise durchgeführten Tätigkeiten oder erbrachten Dienstleistungen stehen und ausreichen, um diese Kosten zu decken. Alle Ausgaben der ENISA für Personal, das an den in den Absätzen 1, 2 und 3 genannten Tätigkeiten beteiligt ist, werden in den zu deckenden Kosten berücksichtigt. Die Höhe der Gebühren wird so festgesetzt, dass sowohl ein Defizit als auch eine erhebliche Anhäufung von Überschüssen im Haushaltsplan der

ENISA vermieden wird. Haushaltsüberschüsse aus Gebühren werden zur Finanzierung der Tätigkeiten der ENISA, insbesondere künftiger Tätigkeiten im Zusammenhang mit Gebühren, oder zum Ausgleich entstandener Verluste übertragen. Ergibt sich aus der Erbringung der durch die Gebühren gedeckten Dienstleistungen wiederholt ein erheblicher positiver Saldo im Haushalt oder aus der Erbringung der durch die Gebühren gedeckten Dienstleistungen ein erheblicher negativer Saldo, so ändert die Kommission die in Absatz 5 genannten Durchführungsrechtsakte, um die Methode zur Berechnung der Gebühren gemäß Artikel 118 Absatz 2 zu überarbeiten.

Die Höhe der Gebühren für die in Absatz 1 genannten Aufgaben wird so festgesetzt, dass die Einnahmen daraus ausreichend zur Deckung der Kosten der Tätigkeiten im Zusammenhang mit der Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, der Bearbeitung von Anträgen und der Erteilung und Verlängerung von Befugnissen sowie der erforderlichen Aufsichtstätigkeiten durch die ENISA beitragen.

Die Höhe der Gebühren für die in Absatz 2 genannten Aufgaben wird so bemessen, dass die Einnahmen hieraus ausreichend zur vollständigen Deckung der Kosten der Tätigkeiten im Zusammenhang mit der Pflege der europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 75 beitragen.

Die Höhe der Gebühren für die in Absatz 3 genannten Aufgaben wird so bemessen, dass die Einnahmen hieraus ausreichend zur Deckung der Kosten der Tätigkeiten im Zusammenhang mit der Bereitstellung von Testinstrumenten gemäß Artikel 15 Absatz 1 beitragen.

(7) Die ENISA legt im Rahmen des Rechnungslegungsverfahrens gemäß Artikel 50 einen Bericht über die erhobenen Gebühren und deren Auswirkungen auf ihren Haushalt vor.

(8) Die ENISA führt eine Reihe von Indikatoren ein, um die Arbeitsbelastung, Wirksamkeit und Effizienz in Bezug auf die durch Gebühren finanzierten Tätigkeiten zu messen. Die ENISA passt ihre Personalplanung und die Verwaltung der Mittel aus Gebühren entsprechend an, um auf eine solche Nachfrage und etwaige Schwankungen bei den Einnahmen aus Gebühren angemessen reagieren zu können. Die ENISA leitet den Bericht an die Kommission weiter, die ihn für die Zwecke der in Artikel 120 Absatz 1 genannten Bewertung verwenden kann.

Artikel 48
Ausführung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor trägt die Verantwortung für die Ausführung des Haushaltsplans der ENISA und fungiert als Anweisungsbefugter.

(2) Der interne Rechnungsprüfer der Kommission übt gegenüber der ENISA dieselben Befugnisse wie gegenüber den Kommissionsdienststellen aus.

(3) Jedes Jahr übermittelt der Exekutivdirektor der Haushaltsbehörde alle Informationen, die für die Ergebnisse von Bewertungsverfahren von Belang sind.

Artikel 49
Rechnungslegung und Entlastung

(1) Bis zum 1. März des jeweils folgenden Haushaltsjahres (Jahr N + 1) übermittelt der Rechnungsführer der ENISA dem Rechnungsführer der Kommission und dem Rechnungshof den vorläufigen Jahresabschluss für das Haushaltsjahr (Jahr N).

(2) Der Rechnungsführer der ENISA übermittelt dem Rechnungsführer der Kommission auf die von Letzterem vorgeschriebene Weise bzw. in dem von ihm vorgeschriebenen Format auch die erforderlichen Rechnungsführungsinformationen zu Konsolidierungszwecken bis zum 1. März des Jahres N + 1.

(3) Die ENISA übermittelt dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof den Bericht über die Haushaltsführung und das Finanzmanagement für das Jahr N bis zum 31. März des Jahres N + 1.

(4) Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Rechnungsabschluss der ENISA für das Jahr N, erstellt der Rechnungsführer der ENISA in eigener Verantwortung den endgültigen Jahresabschluss der ENISA. Der Exekutivdirektor legt ihn dem Verwaltungsrat zur Stellungnahme vor.

(5) Der Verwaltungsrat gibt eine Stellungnahme zum endgültigen Rechnungsabschluss der ENISA für das Jahr N ab.

(6) Der Rechnungsführer der ENISA leitet den endgültigen Rechnungsabschluss für das Jahr N zusammen mit der Stellungnahme des Verwaltungsrats bis zum 1. Juli des Jahres N + 1 dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof zu.

(7) Der endgültige Rechnungsabschluss der ENISA für das Jahr N wird bis zum 15. November des Jahres N + 1 im *Amtsblatt der Europäischen Union* veröffentlicht.

(8) Bis zum 30. September des Jahres N + 1 übermittelt der Exekutivdirektor dem Rechnungshof eine Antwort auf die Bemerkungen in dessen Jahresbericht. Der Exekutivdirektor übermittelt diese Antwort auch dem Verwaltungsrat und der Kommission.

(9) Gemäß Artikel 267 Absatz 3 der Verordnung (EU, Euratom) 2024/2509 des Europäischen Parlaments und des Rates unterbreitet der Exekutivdirektor dem Europäischen Parlament auf dessen Anfrage alle für ein reibungsloses Entlastungsverfahren für das Jahr N notwendigen Informationen.

(10) Auf Empfehlung des Rates, der mit qualifizierter Mehrheit beschließt, erteilt das Europäische Parlament dem Exekutivdirektor vor dem 15. Mai des Jahres N + 2 Entlastung für die Ausführung des Haushaltsplans für das Jahr N.

Artikel 50
Finanzregelung

(1) Der Verwaltungsrat erlässt nach Konsultation der Kommission die für die ENISA geltende Finanzregelung. Die Finanzregelung darf von der Delegierten Verordnung (EU) 2019/715 nur abweichen, wenn dies für den Betrieb der ENISA eigens erforderlich ist und die Kommission vorher ihre Zustimmung erteilt hat.

(2) Die Erstellung und die Ausführung des Haushaltsplans durch die ENISA erfolgen im Einklang mit ihrer Finanzregelung und der Verordnung (EU, Euratom) 2024/2509.

Artikel 51
Betrugsbekämpfung

(1) Zur Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gelten für die Tätigkeiten der ENISA uneingeschränkt die Bestimmungen der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates[75].

(2) Die ENISA tritt der Interinstitutionellen Vereinbarung vom 25. Mai 1999 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF)[76] innerhalb von sechs Monaten nach dem *[Amt für Veröffentlichungen: Bitte genaues Datum nach Artikel 127 einfügen]* bei und erlässt nach dem Muster in der Anlage der Vereinbarung die entsprechenden Bestimmungen, die für ihr Personal gelten.

(3) Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der ENISA erhalten haben, Rechnungsprüfungen anhand von Belegkontrollen und Kontrollen vor Ort durchzuführen.

(4) Das OLAF kann gemäß den Vorschriften und Verfahren der Verordnung (EU, Euratom) Nr. 883/2013 und der Verordnung (Euratom, EG) Nr. 2185/96 des Rates[77] Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit von der ENISA gewährten Finanzhilfen bzw. finanzierten Verträgen ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

(5) Unbeschadet der Absätze 1 bis 4 müssen Arbeitsvereinbarungen mit Drittländern und internationalen Organisationen, Verträge, Finanzhilfevereinbarungen und Finanzhilfeentscheidungen der ENISA Bestimmungen enthalten, die den Rechnungshof und das OLAF ausdrücklich ermächtigen, derartige Rechnungsprüfungen und Untersuchungen im Rahmen ihrer jeweiligen Zuständigkeiten durchzuführen.

(6) Gemäß der Verordnung (EU) 2017/1939 des Rates kann die EUStA Betrug und sonstige rechtswidrige Handlungen zum Nachteil der finanziellen Interessen der Union im Sinne der Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates[78] untersuchen und verfolgen.

---

75 Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1, ELI: http://data.europa.eu/eli/reg/2013/883/oj).

76 ABl. L 136 vom 31.5.1999, S. 15, ELI: http://data.europa.eu/eli/agree_interinstit/1999/531/oj.

77 Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. L 292 vom 15.11.1996, S. 2, ELI: http://data.europa.eu/eli/reg/1996/2185/oj).

78 Richtlinie (EU) 2017/1371 des Europäischen Parlaments und des Rates vom 5. Juli 2017 über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug (ABl. L 198 vom 28.7.2017, S. 29, ELI: http://data.europa.eu/eli/dir/2017/1371/oj).

Artikel 52
Interessenerklärung

(1) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, der stellvertretende Exekutivdirektor und die von den Mitgliedstaaten auf Zeit abgeordneten Beamten geben eine Verpflichtungserklärung und eine Interessenerklärung ab, aus der hervorgeht, ob direkte oder indirekte Interessen bestehen, die ihre Unabhängigkeit beeinträchtigen könnten. Die Erklärungen müssen der Wahrheit entsprechen und vollständig sein; sie werden jedes Jahr schriftlich abgegeben und, wann immer erforderlich, aktualisiert.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, der stellvertretende Exekutivdirektor und externe Sachverständige, die in den Ad-hoc-Arbeitsgruppen mitwirken, geben spätestens zu Beginn jeder Sitzung eine wahrheitsgetreue und vollständige Erklärung über alle Interessen ab, die ihre Unabhängigkeit in Bezug auf die Tagesordnungspunkte beeinträchtigen könnten, und beteiligen sich nicht an den Diskussionen und den Abstimmungen über solche Punkte.

(3) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten der Vorschriften über Interessenerklärungen nach den Absätzen 1 und 2 fest.

Artikel 53
Transparenz

(1) Die ENISA übt ihre Tätigkeiten mit einem hohen Maß an Transparenz und im Einklang mit Artikel 55 aus.

(2) Die ENISA stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu ihren eigenen Arbeitsergebnissen, erhalten. Ferner macht sie die nach Artikel 52 abgegebenen Interessenerklärungen öffentlich zugänglich.

(3) Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Tätigkeiten der ENISA teilnehmen.

(4) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Transparenzregelungen fest.

Artikel 54
Vertraulichkeit innerhalb der ENISA

(1) Unbeschadet des Artikels 55 legt die ENISA Informationen, die bei ihr eingehen oder von ihr verarbeitet werden und die auf begründetes Ersuchen vertraulich behandelt werden sollen, nicht gegenüber Dritten offen.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, der stellvertretende Exekutivdirektor, die Mitglieder der ENISA-Beratungsgruppe, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal der ENISA, einschließlich der von den Mitgliedstaaten auf Zeit abgeordneten Beamten, unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 AEUV.

(3) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Vertraulichkeitsregelungen fest.

Artikel 55
Zugang zu Dokumenten

(1) Die Verordnung (EG) Nr. 1049/2001 findet Anwendung auf die Dokumente der ENISA.

(2) Der Verwaltungsrat legt Maßnahmen zur Durchführung der Durchführungsverordnung (EG) Nr. 1049/2001 fest.

(3) Gegen Entscheidungen der ENISA gemäß Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe des Artikels 228 bzw. 263 AEUV Beschwerde beim Europäischen Bürgerbeauftragten eingelegt oder Klage beim Gerichtshof der Europäischen Union erhoben werden.

KAPITEL V
Personal und Verbindungsbeamte

Artikel 56
Allgemeine Bestimmungen

(1) Für das Personal der ENISA gelten das Statut der Beamten, die Beschäftigungsbedingungen für die sonstigen Bediensteten sowie die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung der Bestimmungen des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten.

(2) Das Personal der ENISA, die Verbindungsbeamten und die zur ENISA abgeordneten nationalen Sachverständigen durchlaufen ein geeignetes Sicherheitsüberprüfungsverfahren.

Artikel 57
Vorrechte und Befreiungen

Das dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf die ENISA und ihr Personal Anwendung.

Artikel 58
Verbindungsbeamte

(1) Jeder Mitgliedstaat benennt gemäß Artikel 59 Absatz 2 mindestens zwei Verbindungsbeamte aus einer gemäß Artikel 8 Absatz 1 der Richtlinie (EU) 2022/2555 benannten zuständigen nationalen Behörde als zur ENISA abgeordnete nationale Sachverständige, die an ihrem Sitz oder ihrer Außenstelle tätig sind. Die Kommission kann ebenfalls einen Verbindungsbeamten benennen.

(2) Die Verbindungsbeamten tragen zur Erfüllung der Aufgaben der ENISA bei, indem sie unter anderem die operative Zusammenarbeit und den Informationsaustausch gemäß Artikel 11 erleichtern. Außerdem unterstützen die Verbindungsbeamten die ENISA dabei, ihre Tätigkeiten, Feststellungen und Empfehlungen bei den

einschlägigen Interessenträgern in der gesamten Union bekannt zu machen. Zudem dienen sie als nationale Kontaktstellen für Fragen aus ihrem jeweiligen Mitgliedstaat und solchen mit Bezug zu ihrem Mitgliedstaat, entweder indem sie diese Fragen direkt beantworten oder sich mit ihren nationalen Verwaltungen in Verbindung setzen.

(3) Die von ihren Mitgliedstaaten benannten Verbindungsbeamten sind dazu befugt, nach strikter Maßgabe des nationalen Rechts oder der Gepflogenheiten des jeweiligen Mitgliedstaats, insbesondere in Bezug auf Datenschutz und Vertraulichkeit, alle einschlägigen Informationen, wie von dieser Verordnung vorgesehen, von ihrem jeweiligen Mitgliedstaat anzufordern und zu erhalten.

Artikel 59
Abgeordnete nationale Sachverständige und sonstiges Personal

(1) Die ENISA kann in allen ihren Tätigkeitsbereichen auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht von der ENISA selbst beschäftigt wird. Für dieses Personal gelten das Beamtenstatut und die Beschäftigungsbedingungen nicht.

(2) Der Verwaltungsrat beschließt eine Regelung über zur ENISA abgeordnete nationale Sachverständige, einschließlich Verbindungsbeamten.

KAPITEL VI
ALLGEMEINE BESTIMMUNGEN FÜR DIE ENISA

Artikel 60
Rechtsform der ENISA

(1) Die ENISA ist eine Einrichtung der Union mit eigener Rechtspersönlichkeit.

(2) Die ENISA besitzt in jedem Mitgliedstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach nationalem Recht des entsprechenden Mitgliedstaats zuerkannt ist. Sie kann insbesondere bewegliches und unbewegliches Vermögen erwerben oder veräußern und ist vor Gericht parteifähig.

(3) Die ENISA wird vom Exekutivdirektor vertreten.

Artikel 61
Sitz

Die ENISA hat ihren Sitz in Athen, Griechenland.

Artikel 62
Sitzabkommen und Arbeitsbedingungen

(1) Die notwendigen Regelungen über die Unterbringung der ENISA in dem Mitgliedstaat, in dem sie ihren Sitz hat, und über die Einrichtungen, die von diesem Mitgliedstaat zur Verfügung zu stellen sind, sowie die besonderen Vorschriften, die im Sitzmitgliedstaat der ENISA für den Exekutivdirektor, die Mitglieder des Verwaltungsrats, das Personal der ENISA und für Familienangehörige dieser Personen gelten, werden in einem Sitzabkommen festgelegt, das nach Billigung

durch den Verwaltungsrat zwischen der ENISA und dem Sitzmitgliedstaat geschlossen wird.

(2) Der Sitzmitgliedstaat der ENISA gewährleistet die bestmöglichen Voraussetzungen für das reibungslose Funktionieren der ENISA, unter Berücksichtigung der Erreichbarkeit des Standortes, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten der Mitglieder des Personals.

Artikel 63
Verwaltungskontrolle

Die Tätigkeit der ENISA unterliegt der Aufsicht des Europäischen Bürgerbeauftragten nach Artikel 228 AEUV.

Artikel 64
Haftung der ENISA

(1) Die vertragliche Haftung der ENISA bestimmt sich nach dem für den betreffenden Vertrag geltenden Recht.

(2) Für Entscheidungen aufgrund einer Schiedsklausel in einem von der ENISA geschlossenen Vertrag ist der Gerichtshof der Europäischen Union zuständig.

(3) Im Bereich der außervertraglichen Haftung ersetzt die ENISA den durch sie selbst oder ihre Bediensteten in Ausübung ihrer Tätigkeit verursachten Schaden nach den allgemeinen Grundsätzen, die den Rechten der Mitgliedstaaten gemeinsam sind.

(4) Für Streitigkeiten über den Schadensersatz nach Absatz 3 ist der Gerichtshof der Europäischen Union zuständig.

(5) Die persönliche Haftung der Bediensteten gegenüber der ENISA bestimmt sich nach den Vorschriften des Beamtenstatuts bzw. der für sie geltenden Beschäftigungsbedingungen.

Artikel 65
Sprachenregelung

(1) Für die ENISA gilt die Verordnung Nr. 1 des Rates[79]. Die Mitgliedstaaten und die anderen von den Mitgliedstaaten benannten Einrichtungen können sich in einer der Amtssprachen der Organe der Union ihrer Wahl an die ENISA wenden und erhalten eine Antwort in dieser Sprache.

(2) Die für das Funktionieren der ENISA benötigten Übersetzungsleistungen und alle sonstigen sprachbezogenen Dienstleistungen mit Ausnahme von Dolmetscherdiensten werden vom Übersetzungszentrum für die Einrichtungen der Europäischen Union erbracht.

[79] Verordnung Nr. 1 des Rates zur Regelung der Sprachenfrage für die Europäische Wirtschaftsgemeinschaft (ABl. 17 vom 6.10.1958, S. 385, ELI: http://data.europa.eu/eli/reg/1958/1(1)/oj).

Artikel 66
Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch die ENISA unterliegt der Verordnung (EU) 2018/1725.

(2) Der Verwaltungsrat beschließt die Durchführungsvorschriften gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2018/1725. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) 2018/1725 durch die ENISA erforderlich sind, festlegen.

Artikel 67
Sicherheitsvorschriften für den Schutz von nicht als Verschlusssache eingestuften vertraulichen Informationen und von Verschlusssachen

In Abstimmung mit der Kommission legt die ENISA die Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von nicht als Verschlusssache eingestuften vertraulichen Informationen und von EU-Verschlusssachen enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443[80] und 2015/444[81] festgelegt sind. Diese Sicherheitsvorschriften betreffen unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung solcher Informationen.

Artikel 68
Zusammenarbeit mit Einrichtungen der Union und nationalen Behörden

(1) Um Kohärenz zu gewährleisten, Synergien zu schaffen und Fragen von gemeinsamem Interesse anzugehen, arbeitet die ENISA in Fragen der Cybersicherheit mit dem CERT-EU und den einschlägigen Einrichtungen der Union zusammen, einschließlich Europol, dem mit der Verordnung (EU) 2021/887 eingerichteten Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und dem gemäß Artikel 68 Absatz 1 der Verordnung (EU) 2016/679 eingerichteten Europäischen Datenschutzausschuss.

(2) Die Zusammenarbeit gemäß Absatz 1 kann durch folgende Maßnahmen erfolgen:

a) den Austausch von Know-how und bewährten Verfahren;

b) die Bereitstellung von Beratung und die Veröffentlichung von Leitlinien zu Fragen im Zusammenhang mit der Cybersicherheit;

c) die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben, nach Konsultation der Kommission.

(3) Die ENISA geht eine strukturierte Zusammenarbeit mit dem CERT-EU ein, insbesondere in den Bereichen Kapazitätsaufbau, operative Zusammenarbeit und langfristige strategische Analysen von Cyberbedrohungen.

---

80 Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41, ELI: http://data.europa.eu/eli/dec/2015/443/oj).

81 Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53, ELI: http://data.europa.eu/eli/dec/2015/444/oj).

(4) Die ENISA arbeitet mit den einschlägigen Marktüberwachungsbehörden und den im Rahmen der Unionsrechtsvorschriften im Bereich der Cybersicherheit, einschließlich der Verordnung (EU) 2024/2847, benannten Aufsichtsbehörden zusammen und tauscht Informationen mit ihnen aus.

Artikel 69
Zusammenarbeit mit Interessenträgern

(1) Soweit dies erforderlich ist, um die Ziele der vorliegenden Verordnung zu erreichen, arbeitet die ENISA mit einschlägigen Interessenträgern zusammen, darunter die Cybersicherheitsbranche, die IKT-Branche, KMU, Einrichtungen, die in den in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren tätig sind, Hersteller, Einführer und Händler von Produkten mit digitalen Elementen im Sinne der Verordnung (EU) 2024/2847, Konformitätsbewertungsstellen, die nach dem europäischen Rahmen für die Cybersicherheitszertifizierung und der Verordnung (EU) 2024/2847 notifiziert wurden, Einrichtungen, die im Bereich der elektronischen Identifizierungsmittel tätig sind, Verbrauchergruppen und wissenschaftliche Sachverständige aus dem Bereich der Cybersicherheit. Zu diesem Zweck kann die ENISA öffentlich-private Partnerschaften einrichten.

(2) Die ENISA unterstützt in Zusammenarbeit mit der Kommission die Zusammenarbeit zwischen den notifizierten Konformitätsbewertungsstellen gemäß Artikel 93. Insbesondere kann sie eine Gruppe notifizierter Konformitätsbewertungsstellen für die Weitergabe bewährter Verfahren einrichten, um Synergien mit anderen einschlägigen Rechtsvorschriften der Union, insbesondere der Verordnung (EU) 2024/2847, zu schaffen.

Artikel 70
Zusammenarbeit mit Drittländern und internationalen Organisationen

(1) Die ENISA kann im Einklang mit den Prioritäten der Union mit den zuständigen Behörden von Drittländern und/oder mit internationalen Organisationen zusammenarbeiten, soweit dies zur Verwirklichung der Ziele dieser Verordnung erforderlich ist. Zu diesem Zweck kann die ENISA, nach vorheriger Genehmigung durch die Kommission, Arbeitsvereinbarungen mit den Behörden von Drittländern und internationalen Organisationen treffen. Diese Arbeitsvereinbarungen begründen keine rechtlichen Verpflichtungen für die Union und ihre Mitgliedstaaten.

(2) Im Einklang mit den in Absatz 1 genannten Prioritäten beschließt der Verwaltungsrat eine Strategie für die Beziehungen zu Drittländern und internationalen Organisationen in Bezug auf Angelegenheiten, für die die ENISA zuständig ist. Die Kommission stellt durch den Abschluss einer entsprechenden Arbeitsvereinbarung mit dem Exekutivdirektor sicher, dass die ENISA im Rahmen ihres Mandats und des bestehenden institutionellen Rahmens handelt.

(3) Zur Unterstützung der Zusammenarbeit mit Drittländern, insbesondere mit Ländern, die sich um den Beitritt zur Union bewerben, kann die ENISA ihre Sachkenntnis im Bereich des Kapazitätsaufbaus insbesondere in folgenden Bereichen einbringen:

a) Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten und -ressourcen;

b) Wachstum und Verbesserung der Fachkräftebasis im Bereich Cybersicherheit, unter anderem durch die Förderung des ECSF und der Systeme europäischer

Einzelbescheinigungen von Cybersicherheitskompetenzen sowie durch die Bereitstellung von Lern- und Fortbildungsmaßnahmen;

c) Unterstützung der Planung und Durchführung von Cybersicherheitsübungen.

(4) Die ENISA steht der Beteiligung von Drittländern, die entsprechende Übereinkünfte mit der Europäischen Union geschlossen haben, an ihren Tätigkeiten offen. Gemäß den einschlägigen Bestimmungen in Übereinkünften zwischen Drittländern und der Union werden – nach vorheriger Genehmigung durch die Kommission – Arbeitsvereinbarungen getroffen, die insbesondere Art, Umfang und Form einer Beteiligung dieser Drittländer an den Tätigkeiten der ENISA festlegen; hierzu zählen auch Bestimmungen über die Beteiligung an den von der ENISA durchgeführten Initiativen, finanzielle Beiträge und Personal. In Personalfragen müssen derartige Arbeitsvereinbarungen in jedem Fall mit dem Statut und den Beschäftigungsbedingungen vereinbar sein.

(5) Die ENISA erstattet dem Rat und der Kommission regelmäßig Bericht über die Durchführung der in den Absätzen 1 und 4 genannten Arbeitsvereinbarungen.

TITEL III

EUROPÄISCHER ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

KAPITEL I
Ziele, Umfang und Verfahren

Artikel 71

Ziele und Umfang des europäischen Zertifizierungsrahmens für die Cybersicherheit

(1) Der europäische Zertifizierungsrahmen für die Cybersicherheit wird eingerichtet, um einen digitalen Binnenmarkt für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und Einrichtungen zu schaffen. Dazu soll er das Cybersicherheitsniveau in der Union erhöhen und einen harmonisierten Ansatz für die europäischen Systeme für die Cybersicherheitszertifizierung sowie eine wirksame Zertifizierung ermöglichen, um die Einhaltung der geltenden Rechtsvorschriften der Union zu erleichtern.

(2) Im europäischen Zertifizierungsrahmen für die Cybersicherheit ist ein Mechanismus festgelegt, mit dem europäische Systeme für die Cybersicherheitszertifizierung geschaffen werden, um zu bescheinigen,

a) dass die nach solchen Systemen bewerteten IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen, um die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten oder der Funktionen oder Dienste, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen;

b) dass verwaltete Sicherheitsdienste, die nach solchen Systemen bewertet wurden, den festgelegten Sicherheitsanforderungen zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten entsprechen, auf die im Zusammenhang mit der Erbringung dieser Dienste

zugegriffen wird bzw. die in diesem Zusammenhang verarbeitet, gespeichert oder übermittelt werden, und dass diese Dienste kontinuierlich mit der erforderlichen Kompetenz, Sachkenntnis und Erfahrung von Personal mit einem hinreichenden und angemessenen Maß an einschlägigen Fachkenntnissen und beruflicher Integrität erbracht werden;

c) dass die Cyberabwehr einer Einrichtung, die nach solchen Systemen bewertet wurde, den festgelegten Cybersicherheitsanforderungen entspricht.

(3) Sofern im Unionsrecht oder in nationalen Rechtsvorschriften nicht anders bestimmt, ist die europäische Cybersicherheitszertifizierung freiwillig.

(4) Ein europäisches Cybersicherheitszertifikat und eine EU-Konformitätserklärung, die im Rahmen des europäischen Zertifizierungsrahmens für die Cybersicherheit ausgestellt wurden, werden automatisch in allen Mitgliedstaaten anerkannt.

Artikel 72
Information und Konsultation der Öffentlichkeit

(1) Mindestens einmal jährlich organisiert die Kommission mit Unterstützung der ENISA eine europäische Versammlung für die Cybersicherheitszertifizierung, zu der Mitglieder der ECCG und andere einschlägige Sachverständige aus den Mitgliedstaaten, einschlägige Sachverständige aus Einrichtungen der Union und einschlägige Interessenträger eingeladen werden, um strategische Prioritäten für die Harmonisierung im Bereich der Cybersicherheitszertifizierung zu erörtern.

(2) Die Kommission unterhält eine eigene Website mit Informationen zu den folgenden Aspekten und aktualisiert diese regelmäßig:

a) europäische Systeme für die Cybersicherheitszertifizierung, deren Entwicklung gemäß Artikel 73 in Auftrag gegeben wurde;

b) strategische Prioritäten für die Harmonisierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten, der Cyberabwehr von Einrichtungen oder Sicherheitsanforderungen des Unionsrechts, einschließlich möglicher Bereiche, für die ein europäisches System für die Cybersicherheitszertifizierung in Auftrag gegeben werden könnte.

(3) Die Kommission macht auf der in Absatz 2 genannten Website die Informationen über ihre Beauftragung der ENISA mit der Ausarbeitung eines möglichen Systems gemäß Artikel 73 und über ihren Beschluss, ein von der ENISA gemäß Artikel 74 Absatz 7 übermitteltes mögliches System anzunehmen, abzulehnen oder einzustellen, öffentlich zugänglich.

(4) Während der Ausarbeitung eines möglichen Systems durch die ENISA gemäß Artikel 74 können das Europäische Parlament und der Rat die Kommission in ihrer Eigenschaft als Vorsitzende der ECCG und die ENISA ersuchen, einschlägige Informationen über den Entwurf eines möglichen Systems vorzulegen. Auf Ersuchen des Europäischen Parlaments oder des Rates kann die ENISA im Einvernehmen mit der Kommission und unbeschadet des Artikels 54 dem Europäischen Parlament und dem Rat relevante Teile des Entwurfs eines möglichen Systems in einer dem erforderlichen Vertraulichkeitsniveau angemessenen Weise und gegebenenfalls in eingeschränkter Form zur Verfügung stellen.

(5) Das Europäische Parlament und der Rat können die Kommission und die ENISA ersuchen, Angelegenheiten zu erörtern, die die Umsetzung der europäischen Systeme

für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten und der Cyberabwehr von Einrichtungen betreffen.

Artikel 73

Aufträge für ein europäisches System für die Cybersicherheitszertifizierung

(1) Die Kommission kann die ENISA beauftragen, ein mögliches System für die Cybersicherheitszertifizierung für IKT-Produkte, -Dienste oder -Prozesse oder verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen auszuarbeiten.

(2) In hinreichend begründeten Fällen kann die ECCG der Kommission vorschlagen, einen Auftrag gemäß Absatz 1 zu erteilen.

(3) In dem in Absatz 1 genannten Auftrag werden der Zweck, der Umfang und die Modalitäten der Erfüllung der einschlägigen Sicherheitsziele und Elemente gemäß den Artikeln 80 und 81 im Einzelnen dargelegt. Der Auftrag enthält auch den Entwicklungsplan des möglichen europäischen Systems für die Cybersicherheitszertifizierung und die einschlägigen technischen Spezifikationen, auf die in dem System Bezug genommen oder die darin festgelegt werden sollen.

(4) Bei der Ausarbeitung des in Absatz 1 genannten Auftrags konsultiert die Kommission die ENISA und die ECCG ordnungsgemäß und berücksichtigt die Standpunkte aller einschlägigen Interessenträger und anderer Einrichtungen der Union, gegebenenfalls einschließlich derjenigen, die nach den Rechtsvorschriften der Union relevant sind, nach denen ein europäisches System für die Cybersicherheitszertifizierung die Einhaltung der Vorschriften nachweist und eine Konformitätsvermutung begründet.

Artikel 74

Ausarbeitung und Annahme europäischer Systeme für die Cybersicherheitszertifizierung

(1) Sofern im Auftrag nichts anderes bestimmt ist, arbeitet die ENISA spätestens zwölf Monate nach Eingang eines Auftrags der Kommission gemäß Artikel 73 ein mögliches europäisches System für die Cybersicherheitszertifizierung aus, das die Anforderungen der Artikel 80 und 81 erfüllt.

(2) Für die Ausarbeitung jedes möglichen Systems setzt die ENISA eine Ad-hoc-Arbeitsgruppe nach Artikel 32 Absatz 6 ein, damit sie der ENISA fachliche Beratung bereitstellt.

(3) Bei der Ausarbeitung des möglichen Systems arbeitet die ENISA eng mit der ECCG zusammen. Die ECCG leistet der ENISA Unterstützung und fachliche Beratung bei der Ausarbeitung des möglichen Systems und gegebenenfalls unterstützender technischer Spezifikationen.

(4) Bei der Ausarbeitung des möglichen Systems, gegebenenfalls einschließlich unterstützender technischer Spezifikationen, konsultiert die ENISA zeitnah die Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses. Die ENISA arbeitet außerdem mit den zuständigen Behörden in den Mitgliedstaaten und mit den einschlägigen Einrichtungen der Union zusammen, um deren fachliche Beratung zur Ausarbeitung des möglichen Systems und gegebenenfalls der unterstützenden technischen Spezifikationen einzuholen.

Wenn die ENISA der Kommission das mögliche System gemäß Absatz 6 vorlegt, erläutert sie, wie sie dem vorliegenden Absatz nachgekommen ist.

(5) Bevor das mögliche System und gegebenenfalls die unterstützenden technischen Spezifikationen der Kommission übermittelt werden, ersucht die ENISA die Mitglieder der ECCG um schriftliche Stellungnahmen zu dem möglichen System. Die Stellungnahmen werden spätestens 30 Tage nach dem Datum des Auftrags vorgelegt. Die ENISA berücksichtigt die Stellungnahmen der ECCG-Mitglieder weitestgehend. Das Fehlen solcher Stellungnahmen hindert die ENISA nicht daran, das mögliche System der Kommission vorzulegen.

(6) Die ENISA übermittelt der Kommission das mögliche System spätestens 60 Tage nach dem Datum des in Absatz 5 genannten Auftrags.

(7) Bei Erhalt des möglichen Systems bewertet die Kommission, ob das System dem Auftrag gemäß Artikel 73 entspricht. Innerhalb von 30 Tagen nach dem Zeitpunkt der Vorlage des möglichen Systems ergreift die Kommission eine der folgenden Maßnahmen:

a) Sie nimmt das mögliche System an;

b) sie verweist das mögliche System zurück an die ENISA zusammen mit einer Begründung dafür und gibt ihr eine Frist von höchstens 90 Tagen, innerhalb deren die ENISA ein überarbeitetes mögliches System vorlegen muss;

c) sie stellt das mögliche System ein.

(8) Verweist die Kommission ein mögliches System gemäß Absatz 7 Buchstabe b zur Überarbeitung zurück an die ENISA, so gelten die Absätze 4, 5 und 7 entsprechend.

(9) Auf der Grundlage des von der ENISA ausgearbeiteten und von der Kommission angenommenen möglichen Systems ist die Kommission befugt, Durchführungsrechtsakte zu erlassen, in denen für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen, die die Anforderungen der Artikel 80 und 81 erfüllen, ein europäisches System für die Cybersicherheitszertifizierung festgelegt wird. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

(10) Die Kommission kann in den in Absatz 9 genannten Durchführungsrechtsakten gemäß den Artikeln 18 und 77 auf die von der ENISA entwickelten technischen Spezifikationen verweisen.

(11) Die Kommission kann die Bedingungen für die internationale Anerkennung europäischer Cybersicherheitszertifikate in den in Absatz 9 genannten Durchführungsrechtsakten gemäß Artikel 87 festlegen.

Artikel 75

Pflege eines europäischen Systems für die Cybersicherheitszertifizierung

(1) Jedes europäisches System für die Cybersicherheitszertifizierung legt eine Systempflegestrategie fest. In der Systempflegestrategie werden die Erwartungen in Bezug auf die Pflegetätigkeiten dargelegt, insbesondere in Bezug auf die im System genannten Normen oder technischen Spezifikationen und das Zusammenwirken mit einschlägigen Interessenträgern.

(2) Die ENISA stellt – in Zusammenarbeit mit der Kommission und mit Unterstützung der ECCG und ihrer einschlägigen Untergruppe für die Systempflege – die Pflege

des europäischen Systems für die Cybersicherheitszertifizierung sicher, auch im Hinblick auf die mögliche Überprüfung solcher Systeme durch die Kommission. Die ENISA arbeitet mit den einschlägigen Einrichtungen der Union und Gruppen in Verbindung mit Systempflegetätigkeiten zusammen und tauscht Informationen mit ihnen aus.

(3) Die ENISA kann die Beteiligung des Privatsektors an der Pflege eines Systems in Form einer Ad-hoc-Arbeitsgruppe im Einklang mit der in Absatz 1 genannten Systempflegestrategie organisieren.

(4) Die Pflegetätigkeiten in Bezug auf europäische Systeme für die Cybersicherheitszertifizierung beinhalten Folgendes:

a) die Ausarbeitung, Aktualisierung und Billigung technischer Spezifikationen und Leitlinien zur Unterstützung des harmonisierten und einheitlichen Betriebs der Systeme;

b) die Ermittlung von Normen oder technischen Spezifikationen, die für das System relevant sind;

c) das Zusammenwirken und gegebenenfalls die Einrichtung von Verbindungen mit einschlägigen Interessenträgern, einschließlich europäischer oder internationaler Normungsorganisationen, auch zum Zweck der Leistung oder Entgegennahme technischer Beiträge;

d) die Abgabe von Empfehlungen an die Kommission zu notwendigen Verbesserungen und Aktualisierungen der Systeme, auch im Hinblick auf eine mögliche Überprüfung der Systeme;

e) den Austausch von Informationen im Zusammenhang mit der praktischen Umsetzung der Systeme zwischen den Mitgliedstaaten;

f) Beiträge zu Mechanismen der gegenseitigen Begutachtung und gegenseitigen Bewertung sowie Analysen der Ergebnisse solcher Bewertungen, um den Betrieb der Systeme zu verbessern und ihre mögliche Überprüfung zu unterstützen.

(5) Die ECCG kann eine Stellungnahme zur Pflege europäischer Systeme für die Cybersicherheitszertifizierung abgeben.

Artikel 76
Bewertung, Überprüfung und Widerruf eines europäischen Systems für die Cybersicherheitszertifizierung

(1) Mindestens alle vier Jahre nach dem Beginn der Anwendung eines europäischen Systems für die Cybersicherheitszertifizierung bewertet die ENISA in Zusammenarbeit mit der für die Systempflege zuständigen Untergruppe der ECCG und unter Berücksichtigung der Rückmeldungen der Interessenträger die Wirkung und die Wirksamkeit dieses Systems. Die ENISA nimmt eine Bewertung vor, indem sie eine Marktanalyse gemäß Artikel 8 Absatz 1 durchführt.

(2) Nach der in Absatz 1 genannten Bewertung kann die Kommission ihre Durchführungsrechtsakte zur Festlegung eines europäischen Systems für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 9 überprüfen oder aufheben.

(3) Bei der Überprüfung oder dem Widerruf europäischer Systeme für die Cybersicherheitszertifizierung konsultiert die Kommission die ENISA, die ECCG

und deren für die Systempflege zuständige Untergruppe und trägt darüber hinaus den Standpunkten der einschlägigen Interessenträger und anderer Einrichtungen der Union Rechnung.

(4) Die ECCG kann eine Stellungnahme zur Überprüfung oder zum Widerruf eines europäische Systems für die Cybersicherheitszertifizierung abgeben. Die Kommission trägt dieser Stellungnahme bei der Überprüfung oder dem Widerruf des europäischen Systems für die Cybersicherheitszertifizierung gebührend Rechnung.

Artikel 77

Technische Spezifikationen in europäischen Systemen für die Cybersicherheitszertifizierung

(1) Die ENISA kann technische Spezifikationen im Hinblick auf ein künftiges europäisches System für die Cybersicherheitszertifizierung oder zur Unterstützung der Pflege eines europäischen Systems für die Cybersicherheitszertifizierung entwickeln.

(2) Die in Absatz 1 dieses Artikels genannten technischen Spezifikationen werden mit Unterstützung der ECCG und ihrer für die Systempflege zuständigen Untergruppe sowie gegebenenfalls der entsprechenden Ad-hoc-Arbeitsgruppe gemäß Artikel 75 Absatz 3 zeitnah entwickelt. Zu diesem Zweck holt die ENISA unter Berücksichtigung der in Artikel 75 Absatz 1 genannten Systempflegestrategie auch Beiträge einschlägiger Interessengruppen ein.

(3) Wird in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 auf technische Spezifikationen Bezug genommen, so werden diese auf der in Artikel 79 genannten Website öffentlich zugänglich gemacht.

(4) In hinreichend begründeten Fällen, insbesondere wenn die technischen Spezifikationen Informationen enthalten, die die Sicherheit zertifizierter IKT-Produkte, -Dienste und -Prozesse, verwalteter Sicherheitsdienste oder die Cyberabwehr von Einrichtungen gefährden könnten, werden sie nur an die Interessenträger weitergegeben, die von den Anforderungen des Systems betroffen sind. Auf solche technischen Spezifikationen darf in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 nicht Bezug genommen werden.

Artikel 78

Erleichterung der Einhaltung des Unionsrechts

(1) Soweit dies in einem bestimmten Rechtsakt der Union so bestimmt ist, wird mit einem Zertifikat, das auf der Grundlage eines europäischen Systems für die Cybersicherheitszertifizierung ausgestellt wurde, die Einhaltung der Vorschriften nachgewiesen und die Vermutung begründet, dass eine Übereinstimmung mit den Anforderungen jenes Rechtsakts gegeben ist.

(2) Bewertungstätigkeiten im Rahmen eines europäischen Systems für die Cybersicherheitszertifizierung müssen mit dem entsprechenden Rechtsakt der Union, in dem der Nachweis der Einhaltung der Vorschriften und die Konformitätsvermutung festgelegt sind, im Einklang stehen. Sind solche Bewertungstätigkeiten in dem entsprechenden Rechtsakt der Union nicht vorgesehen, so werden sie in dem System angegeben. Eine Konformitätsbewertung für die Zertifizierung, die die Vermutung der Konformität mit den in den Rechtsvorschriften

der Union festgelegten Anforderungen begründet, wird von einem Dritten durchgeführt.

(3) Fehlen Harmonisierungsrechtsvorschriften der Union, so kann auch im nationalen Recht festlegt werden, dass ein europäisches System für die Cybersicherheitszertifizierung dafür verwendet werden kann, die Einhaltung der Vorschriften nachzuweisen und die Vermutung zu begründen, dass eine Übereinstimmung mit bestimmten im nationalen Recht festgelegten gesetzlichen Anforderungen gegeben ist.

Artikel 79

Einführung europäischer Systeme für die Cybersicherheitszertifizierung, ENISA-Website und Veröffentlichung von Zertifikaten

(1) Die ENISA organisiert Tätigkeiten zur Förderung der Einführung angenommener europäischer Systeme für die Cybersicherheitszertifizierung, unter anderem durch Pflege der in Absatz 2 genannten Website.

(2) Die ENISA unterhält eine eigene Website mit öffentlichen Informationen zu Folgendem und aktualisiert diese regelmäßig:

a) europäische Systeme für die Cybersicherheitszertifizierung;

b) die mit der Pflege jedes europäischen Systems für die Cybersicherheitszertifizierung verbundenen Gebühren;

c) einschlägige technische Spezifikationen der ENISA;

d) europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, einschließlich Informationen in Bezug auf solche Zertifikate und Erklärungen, die nicht mehr gültig sind, ausgesetzt oder widerrufen wurden oder abgelaufen sind;

e) einschlägige zusätzliche Cybersicherheitsinformationen gemäß Artikel 84;

f) Zusammenfassungen gegenseitiger Begutachtungen gemäß Artikel 89 Absatz 7;

g) technische Spezifikationen, auf die in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 Bezug genommen wird.

(3) Gegebenenfalls werden auf der Website gemäß Absatz 2 auch die nationalen Cybersicherheitszertifizierungssysteme angegeben, die durch ein europäisches System für die Cybersicherheitszertifizierung ersetzt wurden.

KAPITEL II
Inhalt europäischer Systeme für die Cybersicherheitszertifizierung

Artikel 80

Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung

(1) Mit einem europäischen System für die Cybersicherheitszertifizierung werden – soweit zutreffend – die folgenden Sicherheitsziele verfolgt:

a) Gewährleistung, dass IKT-Produkte, -Dienste und -Prozesse sowie verwaltete Sicherheitsdienste durch Voreinstellungen und Technikgestaltung sicher sind;

b) Schutz gespeicherter, übermittelter oder anderweitig verarbeiteter Daten vor einer zufälligen oder unbefugten Speicherung, Verarbeitung oder Offenlegung sowie vor einem zufälligen oder unbefugten Zugriff mithilfe angemessener technischer Mittel unter Berücksichtigung des gesamten Lebenszyklus der IKT-Produkte, -Dienste oder -Prozesse;

c) Schutz der Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer vom Nutzer nicht genehmigten Manipulation oder Veränderung und Meldung von Beschädigungen unter Berücksichtigung des gesamten Lebenszyklus der IKT-Produkte, -Dienste oder -Prozesse;

d) Gewährleistung des Schutzes vor unbefugtem Zugriff mithilfe geeigneter Kontrollmechanismen, darunter u. a. zumindest Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme, und Meldung eines möglicherweise unbefugten Zugriffs;

e) Ermittlung und Dokumentation von Komponenten und Schwachstellen, gegebenenfalls u. a. durch Erstellung einer Software-Stückliste, aus der zumindest die obersten Abhängigkeiten der Produkte hervorgehen;

f) Bereitstellung sicherheitsbezogener Informationen durch Aufzeichnung und Überwachung einschlägiger interner Vorgänge wie Zugang zu Daten, Diensten oder Funktionen, gegebenenfalls mit einem Opt-out-Mechanismus für den Nutzer;

g) Nachprüfung, dass IKT-Produkte, -Dienste und -Prozesse keine bekannten ausnutzbaren Schwachstellen aufweisen;

h) Schutz der Verfügbarkeit wesentlicher und grundlegender Funktionen, auch nach einem Sicherheitsvorfall, einschließlich über Abwehr- und Eindämmungsmaßnahmen gegen Überlastungsangriffe auf Server (Denial-of-Service-Angriffe);

i) Minimierung der negativen Auswirkungen auf die Verfügbarkeit von Diensten, die von anderen Netzen und Geräten bereitgestellt werden, im Falle eines physischen oder technischen Sicherheitsvorfalls;

j) Gewährleistung, dass IKT-Produkte, -Dienste und -Prozesse regelmäßig getestet werden und ihre Sicherheit überprüft wird;

k) Gewährleistung, dass Schwachstellen unverzüglich behandelt und behoben werden, unter anderem durch Sicherheitsaktualisierungen, und dass Informationen über behobene Schwachstellen weitergegeben und veröffentlicht werden, es sei denn, die Risiken der Veröffentlichung überwiegen die Vorteile für die Sicherheit;

l) Gewährleistung, dass eine Strategie für die koordinierte Offenlegung von Schwachstellen vorhanden ist;

m) Erleichterung der Weitergabe von Informationen über mögliche Schwachstellen in IKT-Produkten, -Diensten und -Prozessen;

n) Gewährleistung, dass Sicherheitsaktualisierungen, die zur Behandlung festgestellter Sicherheitsprobleme zur Verfügung stehen, unverzüglich verbreitet werden;

o) Gewährleistung, dass die verwalteten Sicherheitsdienste mit der erforderlichen Kompetenz, Sachkenntnis und Erfahrung erbracht werden, wozu auch gehört, dass das mit der Erbringung dieser Dienste betraute Personal über ein ausreichendes und angemessenes Maß an Fachkenntnissen und Kompetenzen in dem betreffenden Bereich, ausreichende und angemessene Erfahrung und ein Höchstmaß an beruflicher Integrität verfügt;

p) Gewährleistung, dass die IKT-Produkte, -Dienste und -Prozesse, die zur Erbringung der verwalteten Sicherheitsdienste eingesetzt werden, durch Technikgestaltung und Voreinstellungen sicher sind und gegebenenfalls die neuesten Sicherheitsaktualisierungen enthalten sowie keine öffentlich bekannten Schwachstellen aufweisen;

q) Gewährleistung, dass die zertifizierte Einrichtung über geeignete interne Verfahren verfügt, um sicherzustellen, dass die Dienste jederzeit in ausreichender und angemessener Qualität erbracht werden;

r) Gewährleistung, dass die zertifizierte Einrichtung in der Lage ist, Sicherheitsvorfälle zu ermitteln, sich davor zu schützen, sie zu erkennen, darauf zu reagieren und sich von ihnen zu erholen;

s) Gewährleistung, dass die zertifizierte Einrichtung in der Lage ist, die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten;

t) Gewährleistung, dass die zertifizierte Einrichtung ihre operative Integrität und Betriebszuverlässigkeit aufbauen, sicherstellen und überprüfen kann, indem sie direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um für die Sicherheit der Netzwerk- und Informationssysteme zu sorgen, die von der Einrichtung genutzt werden und die kontinuierliche Erbringung von Diensten und deren Qualität, einschließlich bei Störungen, unterstützen;

u) Gewährleistung, dass die zertifizierte Einrichtung in der Lage ist, ein Informationssicherheitsmanagementsystem umzusetzen und zu pflegen;

v) Abwehr aller Ereignisse, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, sowie das von der Einrichtung genutzte Netz- und Informationssystem beeinträchtigen können, und Gewährleistung der kontinuierlichen Erbringung von Diensten und deren Qualität, auch bei Störungen;

w) Gewährleistung, dass die Einrichtung in der Lage ist, für die Sicherheit der Verarbeitung personenbezogener Daten zu sorgen.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 119 delegierte Rechtsakte zur Änderung des Absatzes 1 zu erlassen, mit denen Sicherheitsziele

hinzugefügt oder geändert werden, damit sie den neuesten technologischen Entwicklungen und neuen damit verbundenen Bedrohungen Rechnung tragen, sowie die Befugnis zum Erlass neuer Rechtsvorschriften der Union, in denen der Nachweis der Einhaltung der einschlägigen Cybersicherheitsanforderungen und die Vermutung der Konformität damit mithilfe der europäischen Cybersicherheitszertifizierung festgelegt werden.

(3) Ein europäisches System für die Cybersicherheitszertifizierung von Produkten mit digitalen Elementen im Sinne des Artikels 3 Nummer 1 der Verordnung (EU) 2024/2847 wird im Einklang mit den grundlegenden Cybersicherheitsanforderungen in Anhang I der genannten Verordnung und unter Berücksichtigung der verfügbaren harmonisierten Normen konzipiert.

Artikel 81
Elemente europäischer Systeme für die Cybersicherheitszertifizierung

(1) Ein europäisches System für die Cybersicherheitszertifizierung muss mindestens Folgendes enthalten:

a) den Gegenstand und Anwendungsbereich des Zertifizierungssystems, einschließlich der Art oder Kategorie der erfassten IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste oder der Assets, Dienste und Funktionen der Einrichtung, die unter die Zertifizierung fallen;

b) eine klare Beschreibung des Zwecks des Systems und gegebenenfalls die Angabe der Rechtsvorschriften der Union, in denen die Anforderungen festgelegt sind, für die die europäischen Cybersicherheitszertifikate die Einhaltung der Vorschriften nachweisen und eine Konformitätsvermutung begründen;

c) die Systempflegestrategie, in der das Konzept für die Pflegetätigkeiten gemäß Artikel 75 festgelegt ist;

d) die spezifischen Cybersicherheitsanforderungen, Bewertungskriterien und -methoden für die Bewertung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen sowie Verweise auf internationale, europäische oder nationale Normen, die bei der Bewertung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen angewandt werden, oder – wenn solche Normen nicht verfügbar oder angemessen sind – auf von der ENISA gemäß Artikel 77 ausgearbeitete technische Spezifikationen oder, falls solche Spezifikationen nicht verfügbar sind, auf andere technische Spezifikationen;

e) die maximale Gültigkeitsdauer der nach diesem System ausgestellten europäischen Cybersicherheitszertifikate.

(2) Ein europäisches System für die Cybersicherheitszertifizierung muss mindestens Vorschriften und Bedingungen in Bezug auf Folgendes enthalten:

a) die Überwachung der Einhaltung der mit den europäischen Cybersicherheitszertifikaten oder der EU-Konformitätserklärung verbundenen Anforderungen an IKT-Produkte, -Dienste oder -Prozesse, verwaltete Sicherheitsdienste oder an die Cyberabwehr von Einrichtungen, einschließlich

der Mechanismen für den Nachweis der beständigen Einhaltung der festgelegten Cybersicherheitsanforderungen;

b) die Ausstellung, Bestätigung, den Widerruf und die Verlängerung der europäischen Cybersicherheitszertifikate, die Ausweitung oder Verringerung des Zertifizierungsumfangs sowie die Neuzertifizierung;

c) die Folgen für IKT-Produkte, -Dienste oder -Prozesse, verwaltete Sicherheitsdienste oder Einrichtungen, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, die aber den Anforderungen des Systems nicht genügen;

d) das Vorgehen bei der Meldung und Behandlung bislang nicht erkannter Cybersicherheitsschwachstellen in IKT-Produkten, -Diensten und -Prozessen;

e) Inhalt und Format der europäischen Cybersicherheitszertifikate oder der EU-Konformitätserklärungen, die auszustellen sind;

f) die Dauer der Verfügbarkeit der EU-Konformitätserklärung, der technischen Dokumentation und aller weiteren bereitzuhaltenden Informationen des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder der Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist;

g) alle im Rahmen des Systems eingerichteten Mechanismen der gegenseitigen Bewertung für Behörden oder Stellen, die europäische Cybersicherheitszertifikate gemäß Artikel 85 Absatz 4 ausstellen, unbeschadet der gegenseitigen Begutachtung gemäß Artikel 90;

h) die Vertraulichkeit der Informationen und Daten, von denen alle Beteiligten bei der Ausübung von Aufgaben und Tätigkeiten im Zusammenhang mit der Durchführung der Bestimmungen dieses Titels Kenntnis erhalten;

i) Format und Verfahren, die von den Herstellern oder Anbietern von IKT-Produkten, -Diensten und -Prozessen bei der Bereitstellung und Aktualisierung der ergänzenden Informationen zur Cybersicherheit gemäß Artikel 84 zu befolgen sind; und

j) die Kontinuität der Zertifizierungstätigkeiten in außergewöhnlichen Krisensituationen, die unvermeidbar sind und die Möglichkeit der Anwendung der Vorschriften des Zertifizierungssystems behindern.

(3) Ein europäisches System für die Cybersicherheitszertifizierung muss gegebenenfalls auch Folgendes enthalten:

a) eine oder mehrere Vertrauenswürdigkeitsstufen und die entsprechenden Bewertungsniveaus;

b) Schutzprofile zur Festlegung der Sicherheitsanforderungen, die für eine bestimmte Kategorie von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten gelten;

c) Erweiterungsprofile zur Festlegung zusätzlicher Sicherheitsanforderungen, gegebenenfalls einschließlich der Sicherheitsanforderungen, die in den nationalen Bestimmungen zur Umsetzung des Unionsrechts festgelegt sind;

d) Klarstellung, welche Konformitätsbewertungstätigkeiten, einschließlich Kalibrierung, Prüfung, Zertifizierung und Inspektion, für die

Vertrauenswürdigkeitsstufe „hoch“ oder zum Nachweis der Einhaltung der Vorschriften und zur Begründung der Konformitätsvermutung außerhalb des Europäischen Wirtschaftsraums (EWR) zulässig sind;

e) die Angabe nationaler oder internationaler Systeme für die Cybersicherheitszertifizierung derselben Art oder Kategorie von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen;

f) zusätzliche oder besondere Anforderungen an Konformitätsbewertungsstellen, um deren technische Kompetenz für die Evaluierung der Cybersicherheitsanforderungen zu gewährleisten;

g) für die Zertifizierung erforderliche Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen oder auf andere Weise zur Verfügung zu stellen hat;

h) Siegel oder Kennzeichen und die Bedingungen, unter denen diese verwendet werden können;

i) Bedingungen für die internationale Anerkennung europäischer Cybersicherheitszertifikate gemäß Artikel 87.

(4) Die für das europäische System für die Cybersicherheitszertifizierung festgelegten Anforderungen stehen in Einklang mit den Anforderungen des Unionsrechts.

(5) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung gemeinsamer Grundsätze und Musterbestimmungen für die in den Absätzen 1, 2 und 3 genannten Elemente aller europäischen Systeme für die Cybersicherheitszertifizierung zu erlassen. Soweit angemessen und verfügbar, kann ein europäisches System für die Cybersicherheitszertifizierung Verweise auf diese Grundsätze und Musterbestimmungen enthalten.

(6) Die in Absatz 5 genannten Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen. Bei der Entwicklung oder Überarbeitung der gemeinsamen Grundsätze und Musterbestimmungen für die Elemente europäischer Systeme für die Cybersicherheitszertifizierung konsultiert die Kommission die ENISA und berücksichtigt gegebenenfalls die Standpunkte der ECCG, einschlägiger Interessenträger und anderer einschlägiger Stellen.

Artikel 82

Vertrauenswürdigkeitsstufen und Bewertungsniveaus der europäischen Systeme für die Cybersicherheitszertifizierung

(1) Ein europäisches System für die Cybersicherheitszertifizierung kann für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ angeben. Diese Vertrauenswürdigkeitsstufen müssen im Hinblick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalls in einem angemessenen Verhältnis zu dem Risiko stehen, das mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder mit der Art der Einrichtungen, deren Cyberabwehr Gegenstand einer Zertifizierung ist, und deren Betriebsumgebung verbunden ist.

(2) Europäische Cybersicherheitszertifikate beziehen sich auf die jeweilige Vertrauenswürdigkeitsstufe, die im europäischen System für die Cybersicherheitszertifizierung angegeben ist, nach dem diese Cybersicherheitszertifikate ausgestellt wurden. EU-Konformitätserklärungen beziehen sich auf die Vertrauenswürdigkeitsstufe „niedrig“.

(3) Die jeder Vertrauenswürdigkeitsstufe entsprechenden Sicherheitsanforderungen, einschließlich der entsprechenden Sicherheitskontrollen und der entsprechenden Bewertung, die das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess, der verwaltete Sicherheitsdienst oder die Cyberabwehr von Einrichtungen durchlaufen muss, werden in dem jeweiligen europäischen System für die Cybersicherheitszertifizierung festgelegt.

(4) Das europäische Cybersicherheitszertifikat oder die EU-Konformitätserklärung bezieht sich auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren, einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Cybersicherheitsvorfällen besteht.

(5) Ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung für die Vertrauenswürdigkeitsstufe „niedrig“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste oder -Prozesse, die verwalteten Sicherheitsdienste oder die Cyberabwehr von Einrichtungen, für welche dieses Zertifikat oder diese EU-Konformitätserklärung ausgestellt wird, die entsprechenden Sicherheitsanforderungen, einschließlich der Sicherheitskontrollen, erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, die bekannten Grundrisiken für Sicherheitsvorfälle und Cyberangriffe möglichst gering zu halten. Die durchzuführenden Bewertungstätigkeiten beinhalten mindestens eine Überprüfung der technischen Dokumentation. Ist eine solche Überprüfung nicht geeignet, werden alternative Bewertungstätigkeiten mit gleicher Wirkung durchgeführt.

(6) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „mittel“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste oder -Prozesse, die verwalteten Sicherheitsdienste oder Cyberabwehr von Einrichtungen, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitskontrollen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, bekannte Risiken von Sicherheitsvorfällen und Cyberangriffen sowie das Risiko von Cyberangriffen seitens Akteuren mit begrenzten Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführenden Bewertungstätigkeiten beinhalten mindestens eine Überprüfung, die zeigt, dass keine allgemein bekannten Schwachstellen vorliegen, und eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste oder -Prozesse, verwalteten Sicherheitsdienste oder Einrichtungen die erforderlichen Sicherheitskontrollen ordnungsgemäß durchführen. Falls diese Bewertungstätigkeiten nicht geeignet sind, werden alternative Bewertungstätigkeiten mit gleicher Wirkung durchgeführt.

(7) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „hoch“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste oder -Prozesse, die verwalteten Sicherheitsdienste oder die Cyberabwehr von Einrichtungen, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitskontrollen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, Risiken von Sicherheitsvorfällen und dem neuesten Stand der Technik entsprechenden Cyberangriffen seitens Akteuren mit

umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführenden Bewertungstätigkeiten beinhalten mindestens Folgendes:

a) eine Überprüfung, die zeigt, dass keine allgemein bekannten Schwachstellen vorliegen;

b) eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste, -Prozesse, verwalteten Sicherheitsdienste oder Einrichtungen die erforderlichen Sicherheitskontrollen entsprechend dem neuesten Stand der Technik ordnungsgemäß durchführen;

c) eine Bewertung der Widerstandsfähigkeit der IKT-Produkte, -Dienste und -Prozesse, verwalteten Sicherheitsdienste oder Einrichtungen gegenüber kompetenten Angreifern, gegebenenfalls unter Verwendung von Penetrationstests.

Falls diese Bewertungstätigkeiten nicht geeignet sind, werden alternative Bewertungstätigkeiten mit gleicher Wirkung durchgeführt. Alle Konformitätsbewertungstätigkeiten, einschließlich Kalibrierungen, Prüfungen, Zertifizierungen und Inspektionen, für die Vertrauenswürdigkeitsstufe „hoch“ werden im Europäischen Wirtschaftsraum durchgeführt, sofern in einem europäischen System für die Cybersicherheitszertifizierung nicht anders vorgesehen.

(8) Soll mit einem europäischen System für die Cybersicherheitszertifizierung die Einhaltung eines bestimmten Rechtsakts der Union nachgewiesen und die Konformitätsvermutung begründet werden, so muss ein europäisches Cybersicherheitszertifikat die Gewissheit bieten, dass die zertifizierten IKT-Produkte, -Dienste und -Prozesse, verwalteten Sicherheitsdienste oder die Cyberabwehr von Einrichtungen die entsprechenden Cybersicherheitsanforderungen dieses Rechtsakts erfüllen. Alle Konformitätsbewertungstätigkeiten, einschließlich Kalibrierungen, Prüfungen, Zertifizierungen und Inspektionen, für die Konformitätsvermutung werden im Europäischen Wirtschaftsraum durchgeführt, sofern in einem europäischen System für die Cybersicherheitszertifizierung nicht anders vorgesehen.

(9) Ein europäisches System für die Cybersicherheitszertifizierung kann mehrere Bewertungsniveaus für eine bestimmte Vertrauenswürdigkeitsstufe vorsehen. Jedes Bewertungsniveau entspricht einer der Vertrauenswürdigkeitsstufen.

Artikel 83
Selbstbewertung der Konformität

(1) Ein europäisches System für die Cybersicherheitszertifizierung kann die Durchführung einer Selbstbewertung der Konformität unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder Einrichtungen, deren Cyberabwehr Gegenstand einer Zertifizierung ist, zulassen. Die Selbstbewertung der Konformität ist nur für IKT-Produkte, -Dienste oder -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen mit niedrigem Risiko entsprechend der Vertrauenswürdigkeitsstufe „niedrig“ erlaubt.

(2) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder die Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist, kann eine EU-Konformitätserklärung ausstellen, die bestätigt, dass die Erfüllung der im europäischen System für die

Cybersicherheitszertifizierung festgelegten Anforderungen nachgewiesen wurde. Durch die Ausstellung einer solchen Erklärung übernimmt der Hersteller oder Anbieter oder die Einrichtung die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, der verwaltete Sicherheitsdienst oder die Cyberabwehr den in diesem System festgelegten Anforderungen entspricht.

(3) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder die Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist, hält die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste oder der Cyberabwehr mit dem europäischen System für die Cybersicherheitszertifizierung während des Zeitraums, der in dem entsprechenden System festgelegt ist, für die gemäß Artikel 89 benannte nationale Behörde für die Cybersicherheitszertifizierung bereit. Eine Kopie der EU-Konformitätserklärung ist der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA unverzüglich vorzulegen.

Artikel 84

Ergänzende Informationen über die Cybersicherheit zertifizierter IKT-Produkte, -Dienste und -Prozesse

(1) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, für die eine EU-Konformitätserklärung oder eine europäisches Cybersicherheitszertifikat ausgestellt wurde, macht dem Nutzer folgende ergänzende Cybersicherheitsangaben zugänglich:

a) die Zweckbestimmung des betreffenden IKT-Produkts, -Dienstes oder -Prozesses, einschließlich der vom Hersteller oder Anbieter bereitgestellten Sicherheitsumgebung;

b) Leitlinien und Empfehlungen zur Unterstützung der Nutzer bei der sicheren Konfiguration, der Installation, der Bereitstellung, dem Betrieb und der Wartung der IKT-Produkte oder -Dienste;

c) die Art der vom Hersteller oder Anbieter angebotenen technischen Sicherheitsunterstützung und das Enddatum des Unterstützungszeitraums, in dem die Nutzer die Behebung von Schwachstellen und den Erhalt von Sicherheitsaktualisierungen erwarten können;

d) für den Fall, dass der Hersteller oder Anbieter dem Nutzer eine Software-Stückliste zur Verfügung stellt, Angaben dazu, wo darauf zugegriffen werden kann.

(2) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, für die eine EU-Konformitätserklärung oder eine europäisches Cybersicherheitszertifikat ausgestellt wurde, macht folgende ergänzende Cybersicherheitsangaben der Öffentlichkeit zugänglich:

a) die zentrale Anlaufstelle, bei der Informationen über Schwachstellen gemeldet werden können und entgegengenommen werden und das Konzept für die koordinierte Offenlegung von Schwachstellen zu finden ist;

b) Informationen über beseitigte Schwachstellen, einschließlich einer Beschreibung der Schwachstellen mit Angaben, anhand deren die Nutzer das

betroffene Produkt mit digitalen Elementen, die Auswirkungen der Schwachstellen und ihre Schwere erkennen können, sowie eindeutige und verständliche Informationen, die den Nutzern helfen, die Schwachstellen zu beheben; in hinreichend begründeten Fällen, in denen die Hersteller der Auffassung sind, dass die Risiken der Veröffentlichung die Vorteile in Bezug auf die Sicherheit überwiegen, können sie die Veröffentlichung von Informationen über eine behobene Schwachstelle so lange aufschieben, bis den Nutzern die Möglichkeit gegeben wurde, den entsprechenden Patch anzuwenden.

(3) Die in den Absätzen 1 und 2 aufgeführten Angaben werden in elektronischer Form bereitgestellt und bleiben während der Gültigkeitsdauer und mindestens für einen Zeitraum von fünf Jahren nach Ablauf oder Widerruf des jeweiligen europäischen Cybersicherheitszertifikats oder der EU-Konformitätserklärung verfügbar und werden bei Bedarf aktualisiert.

(4) Die in den Absätzen 1 und 2 genannten Verpflichtungen gelten nicht, wenn die Sicherheit des betreffenden IKT-Produkts, -Dienstes oder -Prozesses beeinträchtigt werden könnte, falls die Informationen öffentlich zugänglich gemacht werden.

KAPITEL III
Governance des europäischen Zertifizierungsrahmens für die Cybersicherheit

Abschnitt 1
Allgemeine Vorschriften und Verwaltung europäischer Systeme für die Cybersicherheitszertifizierung

Artikel 85
Ausstellung europäischer Cybersicherheitszertifikate

(1) Für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen, die auf der Grundlage eines europäischen Systems für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Einhaltung der Anforderungen dieses Systems.

(2) Die in Artikel 91 genannten Konformitätsbewertungsstellen stellen ein europäisches Cybersicherheitszertifikat auf der Grundlage der Kriterien des nach Artikel 74 angenommenen europäischen Systems für die Cybersicherheitszertifizierung aus.

(3) Abweichend von Absatz 2 kann ein europäisches System für die Cybersicherheitszertifizierung vorsehen, dass ein im Rahmen dieses Systems erteiltes europäisches Cybersicherheitszertifikat nur von einer der folgenden öffentlichen Stellen auszustellen ist:

a) einer nationalen Behörde für die Cybersicherheitszertifizierung gemäß Artikel 88, die nach Artikel 91 Absatz 1 als Konformitätsbewertungsstelle akkreditiert ist;

b) einer als Konformitätsbewertungsstelle akkreditierten öffentlichen Stelle nach Artikel 91 Absatz 1.

(4) Ist im Rahmen eines nach Artikel 74 angenommenen europäischen Systems für die Cybersicherheitszertifizierung die Vertrauenswürdigkeitsstufe „hoch“ gefordert oder

ist in einem solchen System etwas anderes festgelegt, so kann das europäische Cybersicherheitszertifikat nach diesem System nur von einer nationalen Behörde für die Cybersicherheitszertifizierung gemäß Artikel 88 oder in den folgenden Fällen von einer Konformitätsbewertungsstelle gemäß Artikel 91 Absatz 1 ausgestellt werden:

a) durch eine Konformitätsbewertungsstelle auf der Grundlage eines Modells der vorherigen Zustimmung oder

b) durch eine Konformitätsbewertungsstelle auf der Grundlage eines Modells der allgemeinen Übertragung.

(5) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung der Verfahren für Modelle der vorherigen Zustimmung oder der allgemeinen Übertragung gemäß Absatz 4 zu erlassen. Bei der Vorbereitung dieser Durchführungsrechtsakte konsultiert die Kommission die ECCG. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die natürliche oder juristische Person, die ihre IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste zur Zertifizierung einreicht, oder die Einrichtung, die einen Antrag auf Zertifizierung ihrer Cyberabwehr stellt, hat der gemäß Artikel 89 benannten nationalen Behörde für die Cybersicherheitszertifizierung – sofern diese Behörde die Stelle ist, die das europäische Cybersicherheitszertifikat ausstellt – oder der in Artikel 91 genannten Konformitätsbewertungsstelle alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen.

(7) Konformitätsbewertungsstellen und gegebenenfalls nationale Behörden für die Cybersicherheitszertifizierung unterrichten die ENISA unverzüglich über ihre Entscheidungen, die sich nach Artikel 94 auf den Status der europäischen Cybersicherheitszertifikate und der EU-Konformitätserklärungen auswirken.

(8) Der Inhaber eines europäischen Cybersicherheitszertifikats unterrichtet die Konformitätsbewertungsstelle und gegebenenfalls die nationale Behörde für die Cybersicherheitszertifizierung gemäß Absatz 7 über etwaige später festgestellte Schwachstellen oder Unregelmäßigkeiten hinsichtlich des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses oder des verwalteten Sicherheitsdienstes oder der Cyberabwehr einer Einrichtung, die sich wahrscheinlich auf die Konformität mit Zertifikat auswirken. Diese Stelle leitet diese Informationen unverzüglich an die betreffende nationale Behörde für die Cybersicherheitszertifizierung weiter und bewertet die Auswirkungen auf das Zertifikat im Einklang mit den Bedingungen des Systems gemäß Artikel 81 Absatz 2 Buchstabe d.

(9) Die Inhaber eines europäischen Cybersicherheitszertifikats dürfen in ihren zertifizierten IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten, die für die Gesamtheit oder Teile davon als wichtige Assets gemäß Artikel 102 eingestuft wurden, keine von Hochrisikoanbietern bereitgestellten IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, verwenden, diese installieren oder anderweitig integrieren.

(10) Ein europäisches Cybersicherheitszertifikat wird für die im jeweiligen europäischen System für die Cybersicherheitszertifizierung festgelegte Dauer erteilt und kann verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt sind.

(11) Die Kommission arbeitet mit den Mitgliedstaaten zusammen, um die Anwendung der Bestimmungen im Zusammenhang mit der Ausstellung europäischer Cybersicherheitszertifikate auch im Hinblick auf die Anwendung von Artikel 100 Absatz 4 Buchstabe b sicherzustellen. Die Konformitätsbewertungsstelle und gegebenenfalls die nationale Behörde für die Cybersicherheitszertifizierung stellen der Kommission auf Anfrage unverzüglich alle Informationen im Zusammenhang mit der Ausstellung der betreffenden europäischen Cybersicherheitszertifikate oder EU-Konformitätserklärungen zur Verfügung.

Artikel 86

Nationale Cybersicherheitszertifizierungssysteme und Cybersicherheitszertifikate

(1) Nationale Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse und die verwalteten Sicherheitsdienste sowie die Cyberabwehr von Einrichtungen, die Gegenstand eines europäischen Systems für die Cybersicherheitszertifizierung sind und in dessen Anwendungsbereich fallen, werden ab dem Zeitpunkt unwirksam, der in dem nach Artikel 74 Absatz 9 erlassenen Durchführungsrechtsakt festgelegt ist. Nationale Systeme für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse und die verwalteten Sicherheitsdienste sowie die Cyberabwehr von Einrichtungen, die nicht Gegenstand eines europäischen Systems für die Cybersicherheitszertifizierung sind und nicht in dessen Anwendungsbereich fallen, können bestehen bleiben.

(2) Die Mitgliedstaaten führen keine neuen nationalen Systeme für die Cybersicherheitszertifizierung oder zugehörige Verfahren für die IKT-Produkte, -Dienste und -Prozesse und die verwalteten Sicherheitsdienste sowie die Cyberabwehr von Einrichtungen ein, die bereits Gegenstand eines europäischen Systems für die Cybersicherheitszertifizierung sind und in dessen Anwendungsbereich fallen.

(3) Vorhandene Zertifikate, die auf der Grundlage nationaler Systeme für die Cybersicherheitszertifizierung ausgestellt wurden, die Gegenstand eines europäischen Systems für die Cybersicherheitszertifizierung sind und in dessen Anwendungsbereich fallen, bleiben bis zum Ende ihrer Geltungsdauer gültig.

(4) Die Mitgliedstaaten unterrichten die Kommission und die ECCG, bevor sie neue nationale Systeme für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten und der Cyberabwehr von Einrichtungen annehmen.

(5) Die Kommission kann einem Mitgliedstaat vorschlagen, ein nationales System für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen zu widerrufen, wenn die Entwicklung eines europäischen Systems für die Cybersicherheitszertifizierung für diese Produkte, Dienste und Prozesse oder die Cyberabwehr bereits gemäß Artikel 73 unter Berücksichtigung des Entwicklungsplans eines solchen Systems in Auftrag gegeben wurde.

Artikel 87

Internationale Anerkennung europäischer Cybersicherheitszertifikate

(1) In Drittländern ausgestellte Zertifikate für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und die Cyberabwehr von Einrichtungen können im

Wege eines Durchführungsrechtsakts oder durch den Abschluss einer Vereinbarung zwischen der Union und dem betreffenden Drittland oder einer internationalen Organisation als den europäischen Cybersicherheitszertifikaten gleichwertig anerkannt werden, wenn die Anforderungen des betreffenden Systems des Drittlandes oder einer internationalen Organisation als den Anforderungen der europäischen Systeme für die Cybersicherheitszertifizierung gleichwertig angesehen werden. Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen. Die Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

(2) Die in Absatz 1 genannten Durchführungsrechtsakte und Vereinbarungen müssen auf den gemäß Artikel 74 Absatz 11 festgelegten Bedingungen für die internationale Anerkennung europäischer Cybersicherheitszertifikate beruhen.

(3) Vereinbarungen über die Anerkennung von in Drittländern ausgestellten Zertifikaten oder der in Absatz 1 genannten Zertifikate internationaler Organisationen werden nur geschlossen, wenn darin auch die europäischen Cybersicherheitszertifikate als den Zertifikaten der Drittländer gleichwertig anerkannt werden.

Artikel 88
Nationale Behörden für die Cybersicherheitszertifizierung

(1) Jeder Mitgliedstaat benennt eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet oder – im Einverständnis mit einem anderen Mitgliedstaat – eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung mit Sitz in diesem anderen Mitgliedstaat als für die Aufsichtsaufgaben im benennenden Mitgliedstaat zuständig.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen der benannten nationalen Behörden für die Cybersicherheitszertifizierung mit. Sofern ein Mitgliedstaat mehr als eine Behörde benennt, teilt er der Kommission auch die Aufgaben mit, die diesen Behörden jeweils zugewiesen wurden.

(3) Jede nationale Behörde für die Cybersicherheitszertifizierung ist im Hinblick auf ihre Organisation, Finanzierungsentscheidungen, Rechtsform und Entscheidungsfindung unabhängig von den Einrichtungen, die sie beaufsichtigt.

(4) Die Tätigkeiten der nationalen Behörden für die Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von europäischen Cybersicherheitszertifikaten im Rahmen dieser Verordnung sind streng von ihren Aufsichtstätigkeiten nach diesem Artikel und Artikel 85 Absatz 4 Buchstaben a und b getrennt, und diese Tätigkeiten werden unabhängig voneinander durchgeführt.

(5) Die Mitgliedstaaten stellen sicher, dass die nationalen Behörden für die Cybersicherheitszertifizierung eine angemessene Ausstattung zur Ausübung ihrer Befugnisse und zur wirksamen und effizienten Wahrnehmung ihrer Aufgaben besitzen.

(6) Nationale Behörden für die Cybersicherheitszertifizierung haben die folgenden Aufgaben:

a) Beteiligung an der ECCG gemäß Artikel 90 Absatz 2;

b) Beaufsichtigung und Durchsetzung der Vorschriften im Rahmen der europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 81 Absatz 2 Buchstabe a zur Gewährleistung der Übereinstimmung der IKT-

Produkte, -Dienste und -Prozesse und der verwalteten Sicherheitsdienste sowie der Cyberabwehr von Einrichtungen mit den Anforderungen der in ihrem jeweiligen Hoheitsgebiet ausgestellten europäischen Cybersicherheitszertifikate in Zusammenarbeit mit Marktüberwachungsbehörden oder Aufsichtsbehörden, einschließlich der zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[82] oder der Verordnung (EU) 2024/2847;

c) in Zusammenarbeit mit den zuständigen Marktüberwachungsbehörden Überwachung der Einhaltung und Durchsetzung der in dieser Verordnung festgelegten Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder Einrichtungen, deren Cyberabwehr zertifiziert wird, die eine Selbstbewertung der Konformität in dem entsprechenden europäischen System für die Cybersicherheitszertifizierung durchführen;

d) unbeschadet des Artikels 91 Absatz 3 aktive Unterstützung der nationalen Akkreditierungsstellen oder anderen einschlägigen Behörden bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung;

e) Zusammenarbeit mit der Kommission, wenn die Zuständigkeit einer Konformitätsbewertungsstelle gemäß Artikel 94 angefochten wird;

f) Überwachung und Beaufsichtigung der Tätigkeiten der in Artikel 85 Absatz 3 genannten öffentlichen Stellen;

g) gegebenenfalls Ermächtigung der Konformitätsbewertungsstellen nach Artikel 93, Überwachung der Befolgung der Vorschriften und Durchsetzung der Pflichten der Konformitätsbewertungsstellen zusammen mit den in den europäischen Systemen für die Cybersicherheitszertifizierung gemäß Artikel 81 Absatz 3 Buchstabe f festgelegten zusätzlichen oder spezifischen Anforderungen und Beschränkung, Aussetzung oder Widerruf bestehender Befugnisse, wenn Konformitätsbewertungsstellen gegen die Anforderungen dieser Verordnung verstoßen;

h) Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf europäische Cybersicherheitszertifikate, die von der nationalen Behörde für die Cybersicherheitszertifizierung ausgestellt wurden, oder in Bezug auf europäische Cybersicherheitszertifikate, die nach Artikel 85 Absatz 4 von Konformitätsbewertungsstellen ausgestellt wurden, oder in Bezug auf EU-Konformitätserklärungen nach Artikel 83 eingereicht werden, Untersuchung des Beschwerdegegenstands in angemessenem Umfang und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;

---

82 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

i) jährliche Übermittlung eines Jahresberichts über ihre Haupttätigkeiten an die Kommission, die ENISA und die ECCG bis jeweils zum 31. März [Jahr des Inkrafttretens + 12 Monate] und Bereitstellung dieser Berichte für das Begutachtungsteam, wenn die nationale Behörde für die Cybersicherheitszertifizierung einer gegenseitigen Begutachtung gemäß Artikel 89 unterliegt;

j) Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung, Marktüberwachungsbehörden oder anderen Behörden; dies beinhaltet auch die Weitergabe von Informationen über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten sowie der Cyberabwehr von Einrichtungen mit den Anforderungen dieser Verordnung oder mit den Anforderungen bestimmter europäischer Systeme für die Cybersicherheitszertifizierung;

k) Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung.

(7) Jede nationale Behörde für die Cybersicherheitszertifizierung hat mindestens die folgenden Befugnisse:

a) Sie kann die Konformitätsbewertungsstellen, die Inhaber europäischer Cybersicherheitszertifikate und die Aussteller von EU-Konformitätserklärungen auffordern, ihr sämtliche Auskünfte zu erteilen, die sie für die Erfüllung ihrer Aufgaben benötigt;

b) sie kann Untersuchungen in Form von Rechnungsprüfungen bei den Konformitätsbewertungsstellen, den Inhabern europäischer Cybersicherheitszertifikate und den Ausstellern von EU-Konformitätserklärungen durchführen, um deren Einhaltung der Anforderungen dieses Titels zu überprüfen;

c) sie kann im Einklang mit dem nationalen Recht geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen, die Inhaber von europäischen Cybersicherheitszertifikaten und die Aussteller von EU-Konformitätserklärungen den Anforderungen dieser Verordnung oder eines europäischen Systems für die Cybersicherheitszertifizierung genügen;

d) sie erhält Zugang zu den Räumlichkeiten von Konformitätsbewertungsstellen und von Inhabern europäischer Cybersicherheitszertifikate zum Zweck der Durchführung von Untersuchungen im Einklang mit dem Unionsrecht oder nationalen Verfahrensvorschriften;

e) sie kann im Einklang mit dem nationalen Recht europäische Cybersicherheitszertifikate widerrufen, die von den nationalen Behörden für die Cybersicherheitszertifizierung oder Konformitätsbewertungsstellen nach Artikel 85 Absatz 4 ausgestellt wurden, wenn diese Zertifikate den Anforderungen dieser Verordnung oder eines europäischen Systems für die Cybersicherheitszertifizierung nicht genügen;

f) sie kann im Einklang mit dem nationalen Recht Sanktionen nach Artikel 97 verhängen und die unverzügliche Beendigung von Verstößen gegen die in dieser Verordnung festgelegten Verpflichtungen anordnen.

(8) Die nationalen Behörden für die Cybersicherheitszertifizierung arbeiten untereinander und mit der Kommission zusammen, indem sie insbesondere

Informationen, Erfahrungen und bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten sowie die Cyberabwehr von Einrichtungen austauschen.

(9) Bis zum [6 Monate nach Inkrafttreten] entwickelt die ENISA in Zusammenarbeit mit der Kommission und der ECCG ein Muster für den in Absatz 6 Buchstabe i genannten Bericht.

Artikel 89
Gegenseitige Begutachtung

(1) Die nationalen Behörden für die Cybersicherheitszertifizierung unterliegen der gegenseitigen Begutachtung.

(2) Die gegenseitige Begutachtung erfolgt auf der Grundlage fundierter und transparenter Bewertungskriterien und -verfahren und erstreckt sich insbesondere auf die Strukturen, Personalressourcen und Verfahren betreffenden Anforderungen sowie auf Aspekte der Vertraulichkeit und Beschwerden.

(3) Die gegenseitige Begutachtung umfasst die Bewertung folgender Aspekte:

a) gegebenenfalls die Frage, ob bei den Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von europäischen Cybersicherheitszertifikaten gemäß dieser Verordnung eine strenge Trennung von den Aufsichtstätigkeiten nach Artikel 88 gewahrt wird und ob diese Tätigkeiten unabhängig voneinander durchgeführt werden;

b) die Verfahren für die Beaufsichtigung und Durchsetzung der Vorschriften für die Überwachung der Übereinstimmung von IKT-Produkten, -Diensten, -Prozessen und verwalteten Sicherheitsdiensten sowie der Cyberabwehr von Einrichtungen mit den europäischen Cybersicherheitszertifikaten nach Artikel 88 Absatz 7 Buchstabe a;

c) die Verfahren für die Überwachung und Durchsetzung der Verpflichtungen der Hersteller oder Anbieter von IKT-Produkten, -Diensten, -Prozessen oder verwalteten Sicherheitsdiensten oder von Einrichtungen, deren Cyberabwehr zertifiziert wird, nach Artikel 88 Absatz 7 Buchstabe b;

d) die Verfahren für die Überwachung, Genehmigung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen.

(4) Die gegenseitige Begutachtung wird einmal alle fünf Jahre durch mindestens zwei nationale Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten und die Kommission durchgeführt. Die ENISA nimmt als Beobachterin ebenfalls an der gegenseitigen Beurteilung teil. Das Begutachtungsteam erstellt den Abschlussbericht und eine Zusammenfassung der gegenseitigen Begutachtung.

(5) In Zusammenarbeit mit der Kommission und der ECCG unterstützt die ENISA die Organisation des Mechanismus der gegenseitigen Begutachtung und der gegenseitigen Begutachtungen selbst, unter anderem durch die Entwicklung einschlägiger Leitlinien und Muster.

(6) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um einen Plan für die gegenseitige Begutachtung festzulegen, der sich auf

einen Zeitraum von mindestens fünf Jahren erstreckt, und darin die Kriterien für die Zusammensetzung des Begutachtungsteams, die Methode für die gegenseitige Begutachtung und den Zeitplan, die Häufigkeit und die übrigen Aufgaben in Verbindung mit der gegenseitigen Begutachtung vorzugeben. Bei der Vorbereitung dieser Durchführungsrechtsakte konsultiert die Kommission die ECCG und die ENISA. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

(7) Der Abschlussbericht, einschließlich etwaiger Leitlinien oder Empfehlungen, und die Zusammenfassung der gegenseitigen Begutachtung werden von der ECCG geprüft, die die Zusammenfassung zur Veröffentlichung auf der in Artikel 79 Absatz 2 genannten Website billigt.

Artikel 90
Europäische Gruppe für die Cybersicherheitszertifizierung

(1) Die Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG) wird eingesetzt.

(2) Die Europäische Gruppe für die Cybersicherheitszertifizierung setzt sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertretern anderer einschlägiger nationaler Behörden zusammen. Ein Mitglied der Europäischen Gruppe für die Cybersicherheitszertifizierung darf nicht mehr als zwei Mitgliedstaaten vertreten.

(3) Die Europäische Gruppe für die Cybersicherheitszertifizierung hat folgende Aufgaben:

a) Sie berät und unterstützt die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung der Vorschriften dieses Titels, in politischen Fragen der Cybersicherheitszertifizierung und bei der Koordinierung von Politikkonzepten;

b) sie berät und unterstützt die Kommission bei der Ausarbeitung von Aufträgen für europäische Systeme für die Cybersicherheitszertifizierung gemäß Artikel 73;

c) sie unterstützt und berät die ENISA bei der Ausarbeitung eines möglichen Systems nach Artikel 74 und technischer Spezifikationen nach Artikel 77 und arbeitet hierbei mit der ENISA zusammen;

d) sie unterstützt und berät die ENISA und die Kommission in Bezug auf Systempflegetätigkeiten gemäß Artikel 75 und arbeitet hierbei mit ihnen zusammen;

e) sie unterstützt und berät die Kommission bei der Überprüfung oder dem Widerruf bestehender europäischer Systeme für die Cybersicherheitszertifizierung nach Artikel 76 und arbeitet hierbei mit ihr zusammen;

f) sie schlägt die Beantragung der Ausarbeitung eines möglichen europäischen Systems für die Cybersicherheitszertifizierung gemäß Artikel 73 Absatz 2 bei der Kommission vor;

g) sie gibt an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung sowie zum Widerruf vorhandener europäischer Systeme für die Cybersicherheitszertifizierung ab;

h) sie prüft die einschlägigen Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung, auch auf nationaler Ebene gemäß Artikel 86, und tauscht Informationen und bewährte Verfahren in Bezug auf Cybersicherheitszertifizierungssysteme aus;

i) sie erleichtert die Zusammenarbeit zwischen den nationalen Behörden für die Cybersicherheitszertifizierung nach den Vorschriften dieses Titels im Wege des Kapazitätsaufbaus und des Informationsaustauschs, insbesondere in Fragen der Cybersicherheitszertifizierung;

j) sie leistet Unterstützung bei der Anwendung des Mechanismus der gegenseitigen Begutachtung gemäß Artikel 89 und der Mechanismen der gegenseitigen Bewertung nach den Regeln, die in einem europäischen System für die Cybersicherheitszertifizierung nach Artikel 81 Absatz 2 Buchstabe g festgelegt wurden;

k) sie erleichtert die Anpassung europäischer Systeme für die Cybersicherheitszertifizierung an international anerkannte Normen, unter anderem im Rahmen der Pflege bestehender europäischer Systeme für die Cybersicherheitszertifizierung, und unterbreitet der ENISA erforderlichenfalls Empfehlungen, sich mit den einschlägigen europäischen oder internationalen Normungsorganisationen in Verbindung zu setzen, um Unzulänglichkeiten oder Lücken in verfügbaren europäischen oder international anerkannten Normen anzugehen.

(4) Die Kommission führt mit Unterstützung der ENISA den Vorsitz der ECCG und nimmt deren Sekretariatsgeschäfte wahr.

(5) Die Kommission kann für jeden der folgenden Zwecke ECCG-Untergruppen einsetzen:

a) zur Prüfung spezifischer Fragen auf der Grundlage eines von der Kommission erteilten Mandats;

b) zur Pflege und Überprüfung der europäischen Zertifizierungssysteme im Einklang mit dieser Verordnung und auf der Grundlage eines von der Kommission erteilten Mandats.

(6) Die Untergruppen erstatten der ECCG Bericht.

(7) Den Vorsitz der Untergruppen führen die Kommission und die ENISA gemeinsam, und die Sekretariatsgeschäfte der Untergruppen werden von der ENISA wahrgenommen.

(8) Auf Vorschlag und in Abstimmung mit der Kommission geben sich die ECCG und ihre Untergruppen durch einfache Mehrheit ihrer Mitglieder eine Geschäftsordnung.

Abschnitt 2
Konformitätsbewertungsstellen

Artikel 91
Zuständigkeit von Konformitätsbewertungsstellen

(1) Die Konformitätsbewertungsstellen werden von den nach der Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen akkreditiert. Diese Akkreditierung wird nur ausgestellt, wenn die Konformitätsbewertungsstelle die in Anhang I der vorliegenden Verordnung aufgeführten Anforderungen erfüllt.

(2) Hat eine nationale Behörde für die Cybersicherheitszertifizierung gemäß der vorliegenden Verordnung ein europäisches Cybersicherheitszertifikat ausgestellt, so wird die Zertifizierungsstelle der nationalen Behörde für die Cybersicherheitszertifizierung nach Absatz 1 als Konformitätsbewertungsstelle akkreditiert.

(3) Die Akkreditierung nach Absatz 1 wird den Konformitätsbewertungsstellen für eine Höchstdauer von fünf Jahren erteilt und kann verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen dieses Artikels weiterhin erfüllt. Die nationalen Akkreditierungsstellen treffen innerhalb einer angemessenen Frist alle angebrachten Maßnahmen, um die nach Absatz 1 erteilte Akkreditierung einer Konformitätsbewertungsstelle zu beschränken, auszusetzen oder zu widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

(4) Bei der Festlegung zusätzlicher oder spezifischer Akkreditierungsanforderungen an ein europäisches System für die Cybersicherheitszertifizierung von IKT-Produkten gemäß Artikel 92 werden gegebenenfalls Synergien mit den Anforderungen an notifizierte Stellen gemäß der Verordnung (EU) 2024/2847 und den Akkreditierungsanforderungen im Rahmen der bereits angenommenen Systeme für die Cybersicherheitszertifizierung angestrebt.

(5) Ist eine Konformitätsbewertungsstelle gemäß der Verordnung (EU) 2024/2847 akkreditiert, so können die zuständigen Behörden die Ergebnisse früherer Akkreditierungsverfahren in Bezug auf sich überschneidende Anforderungen als Nachweise während des Akkreditierungsverfahrens gemäß der vorliegenden Verordnung wiederverwenden.

Artikel 92
Weitere Harmonisierung der Zuständigkeit von Konformitätsbewertungsstellen

(1) Sind in einem europäischen System für die Cybersicherheitszertifizierung zusätzliche oder spezifische Anforderungen gemäß Artikel 81 Absatz 3 Buchstabe f festgelegt, so wird den Konformitätsbewertungsstellen von der gemäß Artikel 88 Absatz 1 benannten nationalen Behörde für die Cybersicherheitszertifizierung die Zulassung erteilt, Aufgaben im Rahmen dieses Systems wahrzunehmen. Eine solche Zulassung wird nur erteilt, wenn die Konformitätsbewertungsstelle akkreditiert wurde und die zusätzlichen oder spezifischen Anforderungen des europäischen Systems für die Cybersicherheitszertifizierung erfüllt.

(2) Beantragt eine Konformitätsbewertungsstelle eine Zulassung gemäß diesem Artikel, so wendet sie sich hierzu an die nationale Behörde für die Cybersicherheitszertifizierung des Mitgliedstaates, in dem sie niedergelassen ist, oder an die nationale Behörde für die Cybersicherheitszertifizierung, auf die dieser Mitgliedstaat nach Artikel 88 Absatz 1 zurückgreift.

(3) In folgenden Fällen kann die Konformitätsbewertungsstelle die Zulassung durch eine andere als die in Absatz 2 genannte nationale Behörde für die Cybersicherheitszertifizierung beantragen:

a) falls die in Absatz 1 genannte nationale Behörde für die Cybersicherheitszertifizierung keine solche beantragte Zulassung für die Konformitätsbewertungstätigkeiten erteilt;

b) falls die in Absatz 1 genannte nationale Behörde für die Cybersicherheitszertifizierung keiner gegenseitigen Begutachtung im Einklang mit Artikel 89 in Bezug auf die Konformitätsbewertungstätigkeiten unterzogen wurde, für die die Zulassung beantragt wurde.

(4) Wird einer nationalen Behörde für die Cybersicherheitszertifizierung ein Antrag nach Absatz 3 vorgelegt, informiert sie die nationale Behörde für die Cybersicherheitszertifizierung des Mitgliedstaates, in dem die beantragende Konformitätsbewertungsstelle niedergelassen ist. In solchen Fällen kann die nationale Behörde für die Cybersicherheitszertifizierung dieses Mitgliedstaats als Beobachterin an der Zulassung teilnehmen.

(5) Eine nationale Behörde für die Cybersicherheitszertifizierung kann eine andere nationale Behörde für die Cybersicherheitszertifizierung ersuchen, Teile der Bewertungstätigkeit zu übernehmen. Die Zulassungsbescheinigung wird in einem solchen Fall von der ersuchenden Behörde ausgestellt.

(6) Die Zulassung nach Absatz 1 ist für einen Zeitraum gültig, der die Gültigkeitsdauer der Akkreditierung nicht überschreitet, und kann verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen nach Absatz 1 weiterhin erfüllt und sofern ihre Akkreditierung ebenfalls verlängert wurde.

(7) Die nationalen Behörden für die Cybersicherheitszertifizierung treffen innerhalb einer angemessenen Frist alle angebrachten Maßnahmen, um die nach Absatz 1 erteilte Zulassung einer Konformitätsbewertungsstelle zu beschränken, auszusetzen oder zu widerrufen, wenn die Voraussetzungen für die Zulassung nicht oder nicht mehr erfüllt sind oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

(8) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung der Verfahren, auch für die grenzüberschreitende Zusammenarbeit, für die Zulassung von Konformitätsbewertungsstellen zu erlassen. Bei der Vorbereitung dieser Durchführungsrechtsakte konsultiert die Kommission die ENISA und die ECCG. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 93
Notifizierung von Konformitätsbewertungsstellen

(1) Für jedes europäische System für die Cybersicherheitszertifizierung notifizieren die nationalen Behörden für die Cybersicherheitszertifizierung eines Mitgliedstaats der Kommission und den anderen Mitgliedstaaten die Konformitätsbewertungsstellen, die akkreditiert und gegebenenfalls nach Artikel 92 zugelassen wurden.

(2) Die nationalen Behörden für die Cybersicherheitszertifizierung führen die Notifizierung gemäß Absatz 1 mithilfe des von der Kommission entwickelten und verwalteten elektronischen Notifizierungsinstruments durch.

(3) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um Einzelheiten, Form und Verfahren für Notifizierungen gemäß Absatz 1 festzulegen, einschließlich des Verfahrens für den Einspruch anderer Mitgliedstaaten während des Notifizierungsverfahrens, der eindeutigen Identifizierung von Konformitätsbewertungsstellen sowie der Einzelheiten in Bezug auf die Einschränkung, die Aussetzung oder den Widerruf einer Notifizierung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 94
Anfechtung der Zuständigkeit von Konformitätsbewertungsstellen

(1) Die Kommission untersucht alle Fälle, in denen sie die Zuständigkeit einer Konformitätsbewertungsstelle in Bezug auf die Erfüllung oder die dauerhafte Erfüllung der für die Stelle geltenden Anforderungen und die Wahrnehmung der entsprechenden Zuständigkeiten durch eine Konformitätsbewertungsstelle anzweifelt oder ihr Zweifel daran zur Kenntnis gebracht werden.

(2) Die nationale Behörde für die Cybersicherheitszertifizierung erteilt der Kommission auf Verlangen sämtliche Auskünfte über die Grundlage für die Notifizierung oder die Aufrechterhaltung der Zuständigkeit der Konformitätsbewertungsstelle.

(3) Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen erlangten sensiblen Informationen vertraulich behandelt werden.

(4) Stellt die Kommission fest, dass eine Konformitätsbewertungsstelle die Voraussetzungen für ihre Notifizierung nicht oder nicht mehr erfüllt, setzt sie die nationale Behörde für die Cybersicherheitszertifizierung davon in Kenntnis und fordert diese auf, die erforderlichen Korrekturmaßnahmen zu treffen, einschließlich eines Widerrufs der Notifizierung, sofern dies nötig ist.

(5) Die Mitgliedstaaten stellen sicher, dass ein Einspruchsverfahren gegen die Entscheidungen der notifizierten Stellen vorgesehen ist.

Artikel 95
Verpflichtung von Konformitätsbewertungsstellen zur Bereitstellung und Aufbewahrung von Informationen

(1) Die Konformitätsbewertungsstellen unterrichten die nationale Behörde für die Cybersicherheitszertifizierung über Folgendes:

a) alle Verweigerungen, Einschränkungen, Aussetzungen und Widerrufe einer Bescheinigung oder eines Zertifikats;

b) alle Umstände mit Auswirkungen auf den Anwendungsbereich und die Bedingungen der Notifizierung gemäß Artikel 93 Absatz 1;

c) alle Auskunftsersuchen über Konformitätsbewertungstätigkeiten, die sie von den Marktüberwachungsbehörden erhalten haben;

d) auf Verlangen alle Konformitätsbewertungstätigkeiten, denen sie im Anwendungsbereich ihrer Notifizierung nachgegangen sind, und welche anderen Tätigkeiten, einschließlich grenzübergreifender Tätigkeiten und Vergabe von Unteraufträgen, sie ausgeführt haben.

(2) Die Konformitätsbewertungsstellen stellen der ENISA auch die in Absatz 1 Buchstabe a genannten Informationen zur Verfügung, um ihr die Erfüllung ihrer Aufgabe gemäß Artikel 79 zu erleichtern.

(3) Im Rahmen dieser Verordnung übermitteln Konformitätsbewertungsstellen den übrigen Konformitätsbewertungsstellen, die ähnliche Konformitätsbewertungstätigkeiten in Bezug auf IKT-Produkte, -Dienste oder -Prozesse, verwaltete Sicherheitsdienste oder Einrichtungen, deren Cyberabwehr zertifiziert wird, nachgehen, unverzüglich die einschlägigen Informationen über negative und auf Verlangen auch über positive Ergebnisse von Konformitätsbewertungen.

(4) Konformitätsbewertungsstellen führen ein Aufzeichnungssystem, das alle Unterlagen und Nachweise enthält, die im Zusammenhang mit jeder von ihnen durchgeführten Bewertung und Zertifizierung erstellt oder entgegengenommen werden. Die Aufzeichnungen werden in sicherer und zugänglicher Weise so lange gespeichert, wie dies für die Zwecke der Zertifizierung erforderlich ist, und mindestens für einen Zeitraum von fünf Jahren nach Ablauf oder Widerruf des jeweiligen europäischen Cybersicherheitszertifikats.

Abschnitt 3
Sonstige Bestimmungen

Artikel 96

Beschwerderecht und Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Natürliche und juristische Personen haben das Recht, bei dem Aussteller eines europäischen Cybersicherheitszertifikats oder – wenn sich die Beschwerde gegen ein von einer Konformitätsbewertungsstelle nach Artikel 85 Absatz 4 ausgestelltes europäisches Cybersicherheitszertifikat richtet – bei der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung eine Beschwerde einzulegen.

(2) Die Behörde oder Stelle, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer über den Stand des Verfahrens und die getroffene Entscheidung sowie über das Recht auf einen wirksamen gerichtlichen Rechtsbehelf nach den Absätzen 3 und 4.

(3) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Bezug auf

a) Entscheidungen einer Behörde oder einer Stelle gemäß Absatz 1, gegebenenfalls auch in Bezug auf die mangelnde Erteilung, Verweigerung der Erteilung oder Anerkennung eines europäischen Cybersicherheitszertifikats, das diese natürliche oder juristische Person innehat bzw. beantragt hat;

b) Untätigkeit im Anschluss an eine Beschwerde bei einer Behörde oder Stelle gemäß Absatz 1.

(4) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats eingeleitet, in dem die Behörde oder Stelle, gegen die der Rechtsbehelf gerichtet ist, ihren Sitz hat.

Artikel 97
Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Titel und bei Verstößen gegen die europäischen Systeme für die Cybersicherheitszertifizierung zu verhängen sind, und treffen alle für die Anwendung der Vorschriften erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und melden ihr etwaige spätere Änderungen.

TITEL IV
SICHERHEIT DER IKT-LIEFERKETTEN

KAPITEL I
Rahmen für vertrauenswürdige IKT-Lieferketten

Artikel 98
Umfang des Rahmens

(1) Der Rahmen für vertrauenswürdige IKT-Lieferketten sieht einen Sicherheitsmechanismus auf Unionsebene vor, um nicht technische Risiken in Sektoren mit hoher Kritikalität und anderen kritischen Sektoren im Sinne der Richtlinie (EU) 2022/2555 anzugehen. Im Rahmen des Mechanismus werden wichtige IKT-Assets in kritischen IKT-Lieferketten ermittelt und geeignete und verhältnismäßige Risikominderungsmaßnahmen für die Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art festgelegt.

(2) Die in diesem Titel festgelegten Verpflichtungen gelten unbeschadet der in Artikel 13 der Verordnung (EU) 2024/2847 und in den nationalen Vorschriften zur Umsetzung des Artikels 21 der Richtlinie (EU) 2022/2555 festgelegten Verpflichtungen.

(3) Die Bestimmungen dieses Kapitels hindern die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau in IKT-Lieferketten gewährleisten, sofern diese Bestimmungen mit ihren Pflichten nach dem Unionsrecht im Einklang stehen.

Artikel 99
Bewertung der Sicherheitsrisiken

(1) Die Kommission oder eine Gruppe von mindestens drei Mitgliedstaaten kann die durch Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzte Kooperationsgruppe (im Folgenden „NIS-Kooperationsgruppe“) ersuchen, die auf Unionsebene koordinierten Sicherheitsrisikobewertungen gemäß Artikel 22 der genannten Richtlinie durchzuführen. Wird im Anschluss an ein solches Ersuchen eine Sicherheitsrisikobewertung durchgeführt, so umfasst sie insbesondere die vorgeschlagene Ermittlung der wichtigen IKT-Assets der jeweiligen IKT-Lieferkette und der wichtigsten Bedrohungsakteure, Risiken und Schwachstellen, die sich auf diese Assets auswirken. Im Rahmen der auf Unionsebene koordinierten Sicherheitsrisikobewertungen werden Risikoszenarien entwickelt und Maßnahmen zur Minderung der ermittelten Risiken vorgeschlagen.

(2) Die auf Unionsebene koordinierten Sicherheitsrisikobewertungen werden innerhalb von sechs Monaten nach dem in Absatz 1 genannten Ersuchen abgeschlossen. Auf Ersuchen der Kommission kann die NIS-Kooperationsgruppe einer kürzeren Frist zustimmen.

(3) Hat die Kommission hinreichenden Grund zu der Annahme, dass eine erhebliche Cyberbedrohung für die Sicherheit der Union in Bezug auf eine IKT-Lieferkette besteht und dass Maßnahmen erforderlich sind, um das reibungslose Funktionieren des Binnenmarkts zu erhalten, so ergreift die Kommission unverzüglich folgende Maßnahmen:

a) Konsultation der Mitgliedstaaten zur Notwendigkeit, eine oder mehrere der in Artikel 103 genannten Risikominderungsmaßnahmen zu ergreifen, und

b) Durchführung einer Sicherheitsrisikobewertung unter Berücksichtigung der Konsultation der Mitgliedstaaten. Die Sicherheitsrisikobewertung umfasst die vorgeschlagene Ermittlung der wichtigen IKT-Assets und der wichtigsten Bedrohungsakteure, Risiken und Schwachstellen, die sich auf diese Assets auswirken. Im Rahmen der Sicherheitsrisikobewertungen werden Risikoszenarien entwickelt und Maßnahmen zur Minderung der ermittelten Risiken vorgeschlagen.

Artikel 100
Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen

(1) Ergibt sich aus der Sicherheitsrisikobewertung gemäß Artikel 99 oder anhand anderer Quellen, wie einer öffentlichen Erklärung im Namen der Union oder eines Mitgliedstaats, dass von einem Drittland schwerwiegende, strukturelle nicht technische Risiken für die IKT-Lieferketten ausgehen, überprüft die Kommission die von diesem Land ausgehende Bedrohung unter Berücksichtigung der folgenden Elemente:

a) das Bestehen von Rechtsvorschriften in dem Drittland, nach denen die ihrer rechtlichen Zuständigkeit unterliegenden Einrichtungen verpflichtet sind, den Behörden dieses Drittlands Informationen über Schwachstellen bei Software oder Hardware zu melden, bevor bekannt wird, dass diese Schwachstellen ausgenutzt wurden;

b) bestehende, mithilfe unabhängiger Quellen nachgewiesene Praktiken in dem Drittland, nach denen die der Rechtshoheit des Drittlands unterliegenden Einrichtungen verpflichtet sind, den Behörden dieses Drittlands Informationen über Schwachstellen bei Software oder Hardware zu melden, bevor bekannt wird, dass diese Schwachstellen ausgenutzt wurden;

c) das Fehlen wirksamer Rechtsbehelfe sowie unabhängiger und demokratischer Kontrollmechanismen, mit denen die festgestellten Sicherheitsbedenken, auch in Bezug auf die unter Buchstabe b genannten bestehenden Praktiken, ausgeräumt werden können;

d) fundierte Informationen über einen oder mehrere Sicherheitsvorfälle, die von Bedrohungsakteuren ausgehen, die von diesem Land aus kontrolliert werden und vom Hoheitsgebiets dieses Landes aus tätig sind und böswillige Cyberaktivitäten oder -kampagnen durchführen, und die mangelnde Fähigkeit oder Bereitschaft des Drittlands, mit der Kommission oder den Mitgliedstaaten

zusammenzuarbeiten, um dem Risiko zu begegnen, das sich aus dem Handlungen solcher Bedrohungsakteuren ergibt;

e) einschlägige Informationen aus auf Unionsebene koordinierten Sicherheitsrisikobewertungen oder Berichten von Mitgliedstaaten oder internationalen Organisationen.

(2) Gelangt die Kommission nach der in Absatz 1 genannten Überprüfung zu dem Schluss, dass von einem Drittland schwerwiegende und strukturelle nicht technische Risiken für IKT-Lieferketten ausgehen, so kann sie dieses Drittland im Wege eines Durchführungsrechtsakts als Land benennen, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

(3) Die Kommission überprüft die gemäß Absatz 2 erlassenen Durchführungsrechtsakte regelmäßig.

(4) Hochrisikoanbieter haben kein Recht darauf,

a) sich an der Entwicklung, Bewertung, Konsultation oder Entscheidung in Bezug auf europäische Normen und Dokumente der europäischen Normung gemäß Artikel 10 Absatz 1 der Verordnung (EU) Nr. 1025/2012 und gemeinsame Spezifikationen gemäß Artikel 27 der Verordnung (EU) 2024/2847 im Bereich der Cybersicherheit zu beteiligen;

b) ein europäisches Cybersicherheitszertifikat nach Titel III zu beantragen oder Inhaber eines solchen Zertifikats zu sein;

c) als Konformitätsbewertungsstelle gemäß Titel III akkreditiert zu werden;

d) die Zulassung als befugter Bescheinigungsanbieter europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Titel II Abschnitt 4 zu beantragen;

e) sich an Verfahren zur Vergabe öffentlicher Aufträge zu beteiligen, die nach den Rechtsvorschriften zur Umsetzung der Richtlinien 2014/24/EU und 2014/25/EU in Bezug auf die Bereitstellung von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die in gemäß Artikel 102 ermittelten wichtigen IKT-Assets verwendet werden sollen, durchgeführt werden;

f) sich an etwaigen Tätigkeiten im Rahmen von Finanzierungsprogrammen und -instrumenten der Union, die in direkter und indirekter Mittelverwaltung gemäß Artikel 136 der Verordnung (EU, Euratom) 2024/2509 und nach sektorspezifischen Vorschriften der Union durchgeführt werden, sowie an allen Finanzierungstätigkeiten der Union, die in geteilter Mittelverwaltung durchgeführt werden, in Bezug auf die Bereitstellung von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die in gemäß Artikel 102 ermittelten wichtigen IKT-Assets verwendet werden sollen, zu beteiligen.

Die für die unter den Buchstaben a bis f genannten Verfahren zuständigen Behörden führen die für die Zwecke dieses Absatzes erforderlichen Bewertungen durch. Die Behörden können sich zu diesem Zweck auch auf die in Artikel 104 genannte Liste stützen.

(5) Hat ein Hochrisikoanbieter bereits ein europäisches Cybersicherheitszertifikat gemäß Titel III erlangt, so widerruft die zuständige Behörde dieses unverzüglich.

Artikel 101
Allgemeiner Sicherheitsmechanismus für IKT-Lieferketten

Hat die NIS-Kooperationsgruppe eine auf Unionsebene koordinierte Sicherheitsrisikobewertung gemäß Artikel 99 Absatz 1 dieser Verordnung durchgeführt oder besteht nach Abschluss des Verfahrens eine erhebliche Cyberbedrohung gemäß Artikel 99 Absatz 3 in Bezug auf eine IKT-Lieferkette, so kann die Kommission Maßnahmen gemäß Artikel 102 und Artikel 103 Absätze 1 und 2 ergreifen.

Artikel 102
Ermittlung wichtiger IKT-Assets

(1) Für den Fall, dass die gemäß Artikel 99 Absatz 1 oder 3 durchgeführte Risikobewertung auf erhebliche Cybersicherheitsrisiken in Bezug auf eine IKT-Lieferkette hindeutet, wird der Kommission die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um die wichtigen IKT-Assets zu ermitteln, die für die Herstellung von Produkten oder die Erbringung von Dienstleistungen durch Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art verwendet werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 dieser Verordnung genannten Prüfverfahren erlassen.

(2) Bei der Ermittlung der in Absatz 1 genannten wichtigen IKT-Assets berücksichtigt die Kommission die folgenden Elemente:

a) ob diese Assets wesentliche und sensible Funktionen für das Funktionieren von Produkten oder Dienstleistungen haben, die von einer Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art hergestellt bzw. erbracht werden;

b) ob Sicherheitsvorfälle, auch solche, die durch ausgenutzte Schwachstellen in Bezug auf diese Assets verursacht werden, zu schwerwiegenden Störungen der IKT-Lieferketten im gesamten Binnenmarkt oder zu einer Datenexfiltration führen können;

c) ob eine Abhängigkeit von einer begrenzten Zahl von Anbietern dieser Assets besteht;

d) die Ergebnisse der in Artikel 99 genannten Risikobewertungen.

Artikel 103
Risikominderungsmaßnahmen in IKT-Lieferketten

(1) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um – soweit dies zur Gewährleistung eines hohen Maßes an Cybersicherheit, Cyberresilienz und Vertrauen in der Union erforderlich ist – festzulegen, dass es bestimmten in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen untersagt ist, von den nach Artikel 104 ermittelten Hochrisikoanbietern bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, in jedweder Form in gemäß Artikel 102 ermittelten wichtigen IKT-Assets zu verwenden, zu installieren oder zu integrieren. Diese Durchführungsrechtsakte sehen angemessene

Übergangszeiträume vor, in denen die Kommission die in Artikel 104 genannte Liste der Hochrisikoanbieter veröffentlicht, sowie zusätzliche Fristen für die schrittweise Entfernung der betreffenden IKT-Komponenten und Komponenten, die entsprechende IKT-Komponenten enthalten. In einem solchen Durchführungsrechtsakt können auch diese IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, festgelegt werden.

(2) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um – soweit dies zur Gewährleistung eines hohen Maßes an Cybersicherheit, Cyberresilienz und Vertrauen in der Union erforderlich ist – festzulegen, dass bestimmten in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen eine oder mehrere der folgenden Risikominderungsmaßnahmen in Bezug auf ihre IKT-Lieferketten und insbesondere auf die nach Artikel 102 ermittelten IKT-Komponenten auferlegt werden, um die in den Sicherheitsrisikobewertungen gemäß Artikel 99 ermittelten Risiken zu mindern:

a) Anwendung der Transparenzanforderungen in Bezug auf die Bereitstellung von Informationen über die Anbieter in der IKT-Lieferkette für wichtige IKT-Assets, die gemäß Artikel 102 benannt wurden, an die zuständige Behörde;

b) Verbot der Übermittlung von Daten an Drittländer und der Datenfernverarbeitung in bzw. aus einem Drittland;

c) von Dritten zu prüfende technische Maßnahmen, einschließlich der

i) geräteinternen Verarbeitung,

ii) spezifischen Segmentierung von Netzsystemen,

iii) Sperrung jeglichen Fernzugriffs oder physischen Zugangs zu wichtigen IKT-Assets,

iv) Deaktivierung nicht wesentlicher Merkmale,

v) operativen Netzüberwachung,

vi) Prüfung von Hard- und Software;

d) Beschränkungen im Zusammenhang mit der operativen Kontrolle, einschließlich der Auslagerung organisatorischer Funktionen an Anbieter verwalteter Dienste;

e) Beschränkungen im Zusammenhang mit den vertraglichen Beziehungen der Einrichtung zu ihren Anbietern;

f) Anforderung, dass der Dienst von Personal betrieben, verwaltet, gepflegt oder unterstützt wird, das von den zuständigen nationalen Behörden geprüft wurde;

g) Diversifizierung der Versorgung mit IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten.

(3) Bei der Einführung der in Absatz 2 genannten Maßnahmen kann die Kommission technische und methodische Anforderung für die Maßnahmen festlegen.

(4) Vor dem Erlass der in den Absätzen 1 und 2 genannten Durchführungsrechtsakte bewertet die Kommission potenzielle Risiken und Abhängigkeiten, insbesondere

a) gegebenenfalls die Höhe des Risikos, das mit der Nutzung, Installation oder Integration der von Hochrisikoanbietern bereitgestellten IKT-Komponenten

oder Komponenten, die entsprechende IKT-Komponenten enthalten, in jeglicher Form in wichtigen IKT-Assets verbunden ist;

b) die potenziellen wirtschaftlichen und gesellschaftlichen Auswirkungen, die die Verpflichtung auf Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art haben kann;

c) die Verfügbarkeit alternativer Anbieter zu den Hochrisikoanbietern;

d) die potenzielle Störung grenzübergreifender wirtschaftlicher und gesellschaftlicher Tätigkeiten, die durch einen Sicherheitsvorfall verursacht wird, der die IKT-Lieferketten einer Einrichtung beeinträchtigt.

(5) Die in den Absätzen 1 und 2 genannten Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen und mindestens alle 36 Monate überprüft.

(6) Unter außergewöhnlichen Umständen, die ein Eingreifen zur Aufrechterhaltung des reibungslosen Funktionierens des Binnenmarkts rechtfertigen, und wenn die Kommission hinreichenden Grund zu der Annahme hat, dass die Verwendung, Installation oder Integration von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, von einer bestimmten Einrichtung, die in einem Drittland niedergelassen ist oder von einem Drittland, Einrichtungen aus einem Drittland oder einem Staatsangehörigen aus einem Drittland kontrolliert wird, ein erhebliches nicht technisches Cybersicherheitsrisiko für die wirtschaftlichen oder gesellschaftlichen Tätigkeiten von mindestens drei Mitgliedstaaten darstellt, konsultiert die Kommission unverzüglich die Mitgliedstaaten zu der Notwendigkeit, Maßnahmen auf Unionsebene zu ergreifen.

(7) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um festzulegen, dass es bestimmten in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen untersagt ist, von einer in Artikel 6 genannten Einrichtung bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, zu verwenden, zu installieren oder zu integrieren. Dazu konsultiert sie die Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten, die von dem Verbot betroffen sein könnten. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen. Darin werden gegebenenfalls angemessene Fristen für die schrittweise Entfernung dieser IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, vorgesehen. In einem solchen Durchführungsrechtsakt können auch die diesem Verbot unterliegenden IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, festgelegt werden. Dieses Verbot gilt auch für IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die von allen Einrichtungen stammen, die von der bestimmten in Absatz 6 genannten Einrichtung kontrolliert werden.

(8) In den in den Absätzen 1, 2 und 7 genannten Durchführungsrechtsakten kann auch festgelegt werden, dass die Risikominderungsmaßnahmen nur für die in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen einer bestimmten Größe gelten.

(9) Artikel 100 Absatz 4 gilt für die bestimmte in Absatz 7 genannte Einrichtung, die in einem Drittland niedergelassen ist oder von einem Drittland, einer Einrichtung oder einem Staatsangehörigen aus einem Drittland kontrolliert wird.

(10) Die gemäß den Absätzen 1, 2 und 7 erlassenen Durchführungsrechtsakte, die für die in Anhang I Nummer 10 der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen gelten, gelten entsprechend für die Organe, Einrichtungen und sonstigen Stellen der Union.

Artikel 104
Ermittlung von Hochrisikoanbietern

(1) Die Kommission erstellt im Wege von Durchführungsrechtsakten Listen von Hochrisikoanbietern, für die die mit den Durchführungsrechtsakten gemäß Artikel 103 Absatz 1 oder Artikel 103 Absatz 7 erlassenen Verbote oder das Verbot gemäß Artikel 111 Absatz 1 gelten.

(2) Dazu nimmt die Kommission eine Bestandsaufnahme der Anbieter vor, die IKT-Komponenten und Komponenten, die IKT-Komponenten enthalten, bereitstellen, die von dem in Absatz 1 genannten Verbot erfasst werden.

Auf dieser Grundlage führt die Kommission eine Anfangsbewertung durch, um festzustellen, welche der erfassten Anbieter möglicherweise in einem gemäß Artikel 100 benannten Drittland niedergelassen sind oder von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert werden. Die Kommission nimmt auch eine erste Bestandsaufnahme der Anbieter vor, die möglicherweise von der in Artikel 103 Absatz 6 genannten Einrichtung kontrolliert werden.

(3) Die Kommission bewertet den Ort der Niederlassung sowie die Eigentums- und Kontrollstruktur der ursprünglich gemäß Absatz 2 Unterabsatz 2 ermittelten Anbieter.

(4) Zur Bewertung gemäß Absatz 3 ist die Kommission berechtigt, die hierfür erforderlichen Auskünfte von den Anbietern zu verlangen. Erteilt der Anbieter die erforderlichen Auskünfte nicht innerhalb der festgelegten Frist, kann die Kommission den Schluss ziehen, dass der Anbieter in einem gemäß Artikel 100 benannten Drittland niedergelassen ist oder von einem solchen Drittland, einer in einem solchen Drittland niedergelassenen Einrichtung oder einem Staatsangehörigen eines solchen Drittlands kontrolliert wird. Führt die Kommission eine Bewertung für die Zwecke des Artikels 103 Absatz 7 durch und erteilt der Anbieter die erforderlichen Auskünfte nicht innerhalb der festgelegten Frist, so kann die Kommission den Schluss ziehen, dass der Anbieter von einer gemäß dem genannten Artikel benannten Einrichtung kontrolliert wird. Die in Artikel 112 genannten zuständigen Behörden geben auf Verlangen einschlägige Informationen an die Kommission weiter.

(5) Die Kommission teilt dem betreffenden Anbieter die vorläufigen Feststellungen in Bezug auf die Bewertung der Niederlassung, der Kontrolle und der Eigentumsverhältnisse mit. Die Kommission gibt dem Anbieter Gelegenheit, zu den vorläufigen Feststellungen angehört zu werden.

(6) Die Kommission kann eine zuständige Behörde ersuchen, die Anfangsbewertung der Niederlassung, Eigentumsverhältnisse und Kontrolle eines Anbieters vorzunehmen, wenn dies angesichts der Merkmale der Tätigkeit dieses Anbieters gerechtfertigt ist. Eine zuständige Behörde kann anbieten, eine solche Anfangsbewertung durchzuführen. Die Kommission überprüft diese ersten Feststellungen, um zu

entscheiden, ob der Anbieter in die Liste der Hochrisikoanbieter aufgenommen werden sollte.

(7) Die Kommission aktualisiert die Liste der Hochrisikoanbieter regelmäßig, indem sie Hochrisikoanbieter streicht oder hinzufügt. In der Liste aufgeführte Hochrisikoanbieter können die Kommission ersuchen, ihre Niederlassung und ihre Kontroll- und Eigentumsstruktur neu zu bewerten, wenn sie nachweisen, dass es relevante Änderungen gegeben hat.

(8) Stellt eine zuständige Behörde – auch auf der Grundlage von Informationen, die von einer Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art bereitgestellt werden – fest, dass ein Anbieter möglicherweise in eine Liste der Hochrisikoanbieter aufgenommen werden muss, so unterrichtet sie unverzüglich die Kommission.

Artikel 105

Ausnahmen für Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert werden

(1) Eine Einrichtung, die in einem gemäß Artikel 100 benannten Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen ist oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert wird, kann bei der Kommission einen begründeten Antrag stellen, von Folgendem ausgenommen zu werden:

a) dem Verbot für Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art, ihre IKT-Komponenten oder Komponenten, die ihre IKT-Komponenten enthalten, in jedweder Form in wichtigen IKT-Assets dieser Einrichtungen zu verwenden, zu installieren oder zu integrieren, abweichend von Artikel 111 oder von gemäß Artikel 103 Absatz 1 erlassenen Durchführungsrechtsakten;

b) dem Verbot der Teilnahme an Verfahren zur Vergabe öffentlicher Aufträge, die nach den Rechtsvorschriften zur Umsetzung der Richtlinie 2014/24/EU und der Richtlinie 2014/25/EU in Bezug auf die Bereitstellung von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, die in gemäß Artikel 102 bestimmten wichtigen IKT-Assets verwendet werden sollen, durchgeführt werden, abweichend von Artikel 100 Absatz 4.

(2) Der Antrag nach Absatz 1 enthält folgende Angaben:

a) eine Erläuterung des Interesses der Einrichtung, die in einem gemäß Artikel 100 benannten Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen ist oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert wird, an der Gewährung einer Ausnahme gemäß Absatz 1 und

b) einen eindeutigen Nachweis, dass wirksame Risikominderungsmaßnahmen ergriffen werden, um nicht technische Risiken zu mindern und sicherzustellen, dass das gemäß Artikel 100 benannte Drittland keine unzulässige Einflussnahme in Bezug auf die Bereitstellung von IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, für die Verwendung, Installation oder Integration in wichtigen IKT-Assets einer

Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art ausübt.

(3) Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um die in Absatz 2 Buchstabe b genannten Bedingungen weiter zu präzisieren und Durchführungsbestimmungen für die in diesem Artikel genannten Verfahren festzulegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

(4) Die Kommission bewertet den in Absatz 1 genannten Antrag im Rahmen eines fairen und transparenten Verfahrens und berücksichtigt dabei Folgendes:

a) die in Artikel 100 Absätze 1 und 2 genannten Umstände und zusätzlichen Elemente in Bezug auf das benannte Land, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen und in dem die Einrichtung niedergelassen ist oder von wo aus sie kontrolliert wird;

b) die Wirksamkeit der Risikominderungsmaßnahmen gemäß Absatz 2 Buchstabe b;

c) ob die Ausnahme für die Einrichtung, die in einem Drittland, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen, niedergelassen ist oder von Einrichtungen aus diesem Drittland kontrolliert wird, den Interessen der Union nicht abträglich wäre.

(5) Gelangt die Kommission nach der Bewertung gemäß Absatz 3 zu dem Schluss, dass es gerechtfertigt ist, eine Ausnahme zu gewähren, so erlässt sie einen entsprechenden Beschluss, den sie dem Antragsteller innerhalb von neun Monaten nach Eingang des Antrags mitteilt.

(6) Beim Erlass eines Beschlusses nach Absatz 4 kann die Kommission die Ausnahme auf einen bestimmten Zeitraum beschränken und sie an Bedingungen für die Einrichtung knüpfen, einschließlich

a) eines Zeitplans für die Umsetzung von Risikominderungsmaßnahmen gemäß Absatz 2 Buchstabe b;

b) regelmäßiger Prüfungen durch Dritte, um die wirksame Umsetzung von Risikominderungsmaßnahmen sicherzustellen;

c) Meldepflichten in Bezug auf die Befolgung der Vorschriften.

(7) Gelangt die Kommission nach der Bewertung gemäß Absatz 3 zu dem Schluss, dass es nicht gerechtfertigt ist, eine Ausnahme zu gewähren, so erlässt sie einen entsprechenden Beschluss, den sie dem Antragsteller innerhalb von neun Monaten nach Eingang des Antrags mitteilt.

(8) Die Kommission kann den in Absatz 4 genannten Beschluss von sich aus in einer oder mehreren der folgenden Situationen widerrufen oder ändern:

a) Der Sachverhalt, auf den sich der Beschluss stützte, hat sich in einem wesentlichen Punkt geändert;

b) die Einrichtung, die die Ausnahme beantragt hat, verstößt gegen ihre Verpflichtungen;

c) die Ausnahme beruhte auf unvollständigen, unrichtigen oder irreführenden Angaben der antragstellenden Einrichtung.

Artikel 106
Verteidigungsrechte

Die Kommission stellt sicher, dass vor dem Erlass eines Durchführungsrechtsakts nach Artikel 103 Absatz 7 oder vor dem Erlass eines Beschlusses zur Verweigerung der Gewährung einer Ausnahme nach Artikel 105 Absatz 7 auf der Grundlage von Elementen, die der Antragsteller nicht vorgelegt hat, oder vor dem Widerruf eines Beschlusses nach Artikel 105 Absatz 8 der betreffenden Einrichtung Gelegenheit gegeben wird, sich zu äußern, wobei sie in einigen Fällen der Notwendigkeit eines Dringlichkeitsverfahrens Rechnung trägt.

Artikel 107
Register

Die Kommission führt ein öffentlich zugängliches Register ihrer in Artikel 105 Absatz 5 genannten Beschlüsse. Das Register enthält die Namen der Einrichtungen, die Gegenstand solcher Beschlüsse sind. Die Kommission aktualisiert das Register regelmäßig.

Artikel 108
Vertraulichkeit

Die gemäß den Artikeln 105 und 106 von der Kommission eingeholten Informationen dürfen nur zu dem Zweck verwendet werden, zu dem sie eingeholt wurden.

Artikel 109
Gebühren

(1) Die Kommission kann für Anträge gemäß Artikel 105 Absatz 1 Gebühren erheben.

(2) Gebühren werden in Euro angegeben und entrichtet.

(3) Die Gebühren müssen in einem angemessenen Verhältnis zu den Kosten stehen, die durch die Bearbeitung der in Artikel 105 Absatz 1 genannten Ersuchen, die Bewertung der in Artikel 105 Absatz 2 genannten Kriterien und Informationen sowie die Einrichtung, die Pflege und den Betrieb des in Artikel 107 genannten Registers entstehen. Diese Kosten enthalten alle Ausgaben der Kommission für Personal, das an diesen Tätigkeiten beteiligt ist.

(4) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung von Durchführungsbestimmungen über die Gebühren, in denen die Höhe der Gebühren und die Art und Weise ihrer Entrichtung präzisiert werden. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.

KAPITEL II
IKT-Lieferketten in elektronischen Kommunikationsnetzen

Artikel 110
Wichtige IKT-Assets für mobile, feste und satellitengestützte elektronische Kommunikationsnetze

(1) Die wichtigen IKT-Assets für mobile, feste und satellitengestützte elektronische Kommunikationsnetze sind in Anhang II festgelegt.

(2) Von Hochrisikoanbietern bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, werden schrittweise aus den wichtigen IKT-Assets von mobilen, festen und satellitengestützten elektronischen Kommunikationsnetzen entfernt.

(3) Der Zeitraum für die schrittweise Entfernung der von Hochrisikoanbietern bereitgestellten IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, aus mobilen elektronischen Kommunikationsnetzen darf 36 Monate ab der Veröffentlichung der in Artikel 104 genannten und für die mobilen elektronischen Kommunikationsnetze relevanten Liste der Hochrisikoanbieter nicht überschreiten.

(4) Der Kommission wird die Befugnis übertragen, gemäß Artikel 118 Absatz 2 Durchführungsrechtsakte zu erlassen, um die Fristen für die schrittweise Entfernung der von Hochrisikoanbietern bereitgestellten IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, aus festen und satellitengestützten elektronischen Kommunikationsnetzen festzulegen.

(5) Der Kommission wird die Befugnis übertragen, gemäß Artikel 119 delegierte Rechtsakte zur Änderung des Anhangs II dieser Verordnung zu erlassen, um ihn unter Berücksichtigung der in Artikel 103 Absatz 4 genannten Elemente an die technologischen Entwicklungen anzupassen.

Artikel 111
Verbote für mobile, feste und satellitengestützte elektronische Kommunikationsnetze

(1) Anbieter von mobilen, festen und satellitengestützten elektronischen Kommunikationsnetzen dürfen in keiner Form von Hochrisikoanbietern bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, beim Betrieb der in Anhang II genannten wichtigen IKT-Assets verwenden, installieren oder integrieren.

(2) Falls die gemäß dieser Verordnung benannte zuständige Behörde in einem Mitgliedstaat von der gemäß der Verordnung (EU) XX/XXXX [DNA-Vorschlag] zuständigen Behörde unterscheidet, unterrichtet die gemäß dieser Verordnung benannte zuständige Behörde die gemäß der Verordnung (EU) XX/XXXX [DNA-Vorschlag] zuständige Behörde unverzüglich über die Maßnahmen, die Anbietern von mobilen, festen und satellitengestützten elektronischen Kommunikationsnetzen gemäß Artikel 114 auferlegt wurden. Die Behörden sorgen für eine enge Zusammenarbeit, um eine wirksame Beaufsichtigung und Durchsetzung dieser Maßnahmen zu gewährleisten.

KAPITEL III
Zuständige Behörden, Beaufsichtigung und Durchsetzung, rechtliche Zuständigkeit, Verteidigungsrechte

Artikel 112
Zuständige Behörden

(1) Die Mitgliedstaaten benennen die in Artikel 8 der Richtlinie (EU) 2022/2555 genannten zuständigen Behörden als für das Ergreifen von Aufsichts- und Durchsetzungsmaßnahmen gemäß Artikel 114 verantwortlich.

(2) Die zuständigen Behörden sind strukturell und funktional vollkommen unparteiisch und frei von jeglicher direkter oder indirekter externer Einflussnahme; insbesondere dürfen sie Weisungen von anderen Behörden oder von privater Seite weder einholen noch entgegennehmen.

(3) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden über angemessene Befugnisse, ausreichende personelle und technische Ressourcen sowie die einschlägige Sachkenntnis verfügen, um die Aufsichts- und Durchsetzungsmaßnahmen gemäß Artikel 114 effizient durchzuführen.

(4) Die Mitgliedstaaten notifizieren der Kommission unverzüglich die Namen der gemäß Absatz 1 benannten zuständigen Behörden, die jeweiligen Aufgaben dieser Behörden sowie etwaige spätere Änderungen dieser Angaben. Außerdem veröffentlichen die Mitgliedstaaten die Namen der gemäß Absatz 1 benannten zuständigen Behörden.

Artikel 113
Netz für die Zusammenarbeit und Unterstützungsdienste der Kommission

Zur wirksamen Beaufsichtigung richtet die Kommission ein Netz für die Zusammenarbeit der in Artikel 112 genannten zuständigen Behörden der Mitgliedstaaten und der Kommission ein, das als Plattform für die Zusammenarbeit und den Informationsaustausch dient, insbesondere für die Zwecke der Erstellung von Listen, der Kontrolle und der Bewertung der Eigentumsverhältnisse gemäß Artikel 104. Die Kommission stellt dem Netz administrative Unterstützung bereit.

Artikel 114
Aufsichts- und Durchsetzungsmaßnahmen

(1) Die in Artikel 112 genannten zuständigen Behörden sind befugt, Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art zu ergreifen. Die Mitgliedstaaten stellen sicher, dass die vorstehenden Maßnahmen wirksam, verhältnismäßig und abschreckend sind, wobei jeweils die Umstände des Einzelfalls zu berücksichtigen sind. Die Mitgliedstaaten notifizieren der Kommission die zu diesem Zweck erlassenen Vorschriften und deren spätere Änderungen.

(2) Bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art sind die zuständigen Behörden befugt, diese Einrichtungen folgenden Maßnahmen zu unterziehen:

a) Anforderung einer detaillierten und aktuellen Liste ihrer einschlägigen Anbieter und Dienstleister;

b) Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Überprüfung der Einhaltung dieser Verordnung erforderlich sind;

c) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführter Stichprobenkontrollen;

d) Anforderung von Informationen in Bezug auf die Zusammensetzung von Hardware- oder Softwareprodukten, die in irgendeiner Form in dem Netz oder System installiert oder integriert sind, einschließlich Komponenten und transitiver Abhängigkeiten, in einem gängigen und maschinenlesbaren Format.

(3) Bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art sind die zuständigen Behörden befugt,

a) unter Angabe der maßgeblichen Fakten und rechtlichen Erwägungen Warnungen über Verstöße gegen diese Verordnung durch die betreffenden Einrichtungen herauszugeben;

b) Beschlüsse zu erlassen, mit denen die betreffenden Einrichtungen aufgefordert werden, die Verstöße gegen diese Verordnung oder die bei der Umsetzung von Risikominderungsmaßnahmen festgestellten Mängel zu beheben;

c) die betreffenden Einrichtungen anzuweisen, die gegen diese Verordnung verstoßenden Tätigkeiten einzustellen und von Wiederholungen abzusehen; und

d) gemäß nationalem Recht Geldbußen im Einklang mit den Vorschiften in Bezug auf den in Artikel 115 festgelegten Betrag zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(4) Bei der Ergreifung von im vorangehenden Absatz genannten Durchsetzungsmaßnahmen tragen die zuständigen Behörden den Umständen des Einzelfalls Rechnung und berücksichtigen dabei gebührend zumindest folgende Faktoren:

a) die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde;

b) die Dauer des Verstoßes;

c) die Umsätze der betreffenden Einrichtung;

d) einschlägige frühere Verstöße der betreffenden Einrichtung;

e) gegebenenfalls den durch den Verstoß verursachten materiellen oder immateriellen Schaden, darunter finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Einrichtungen und die Zahl der betroffenen Nutzer;

f) etwaigen Vorsatz oder etwaige Fahrlässigkeit der betreffenden Einrichtung;

g) von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens;

h) den Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit den zuständigen Behörden.

Für die Zwecke von Unterabsatz 1 Buchstabe a gilt Folgendes als schwerer Verstoß:

i) wiederholte Verstöße;

j) Unterlassung der Meldung oder Behebung erheblicher Sicherheitsvorfälle;

k) Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden.

(5) Bevor sie Durchsetzungsmaßnahmen ergreifen, teilen die zuständigen Behörden den betreffenden Einrichtungen ihre vorläufigen Feststellungen mit. Den betreffenden Einrichtungen wird eine angemessene Frist zur Stellungnahme zu den vorläufigen Feststellungen eingeräumt. Die zuständigen Behörden müssen ihre Durchsetzungsmaßnahmen ausführlich begründen.

(6) Die zuständigen Behörden wahren die Grundsätze der Vertraulichkeit und des Berufs- und Geschäftsgeheimnisses.

(7) Die zuständigen Behörden arbeiten im Einklang mit Artikel 116 für Aufsichts- und Durchsetzungszwecke nach diesem Titel miteinander und mit der Kommission zusammen.

Artikel 115
Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diese Verordnung zu verhängen sind, und treffen alle für die Anwendung der Vorschriften erforderlichen Maßnahmen.

(2) Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

(3) Sanktionen werden zusätzlich zu jeglichen der Maßnahmen nach Artikel 114 Absatz 3 Buchstaben a, b und c verhängt.

(4) Bei der Entscheidung über die Verhängung einer Sanktion und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 114 Absatz 4 Unterabsatz 1 genannten Faktoren gebührend zu berücksichtigen.

(5) Verstöße gegen Artikel 103 Absatz 2 Buchstabe a werden – im Einklang mit Absatz 3 des vorliegenden Artikels – mit Sanktionen in Höhe von höchstens 1 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die Einrichtung angehört, belegt.

(6) Verstöße gegen Artikel 103 Absatz 2 Buchstaben b bis g werden – im Einklang mit Absatz 3 des vorliegenden Artikels – mit Sanktionen in Höhe von höchstens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die Einrichtung angehört, belegt.

(7) Verstöße gegen Artikel 103 Absatz 1 und Artikel 111 werden – im Einklang mit Absatz 3 des vorliegenden Artikels – mit Sanktionen in Höhe von höchstens 7 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die Einrichtung angehört, belegt.

Artikel 116
Amtshilfe

(1) Wenn eine Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art ihre Dienste in mehr als einem Mitgliedstaat erbringt oder wenn sie ihre Dienste in einem oder mehreren Mitgliedstaaten erbringt und sich ihre wichtigen IKT-Assets in einem oder mehreren anderen Mitgliedstaaten befinden, so arbeiten die zuständigen Behörden der betreffenden Mitgliedstaaten miteinander und mit der Kommission zusammen und unterstützen einander und die Kommission, um die wirksame und effiziente Anwendung der Verordnung sicherzustellen. Zu diesem Zweck gelten mindestens die folgenden Vorschriften:

a) Die zuständigen Behörden, die in einem Mitgliedstaat Aufsichts- oder Durchsetzungsmaßnahmen ergreifen, unterrichten die zuständigen Behörden in den anderen betreffenden Mitgliedstaaten über die Aufsichts- und Durchsetzungsmaßnahmen und konsultieren sie zu diesen;

b) eine zuständige Behörde in einem Mitgliedstaat kann eine andere zuständige Behörde in einem anderen Mitgliedstaat ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen;

c) eine zuständige Behörde in einem Mitgliedstaat leistet auf begründetes Ersuchen einer anderen zuständigen Behörde in einem anderen Mitgliedstaat der ersuchenden Behörde nach besten Kräften Amtshilfe, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können.

(2) Die in Absatz 1 Buchstabe c genannte Amtshilfe kann Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen, externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen. Die ersuchte zuständige Behörde darf das Amtshilfeersuchen nur ablehnen, wenn festgestellt wird, dass sie für die erbetene Amtshilfe nicht zuständig ist, dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde steht oder dass das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, deren Offenlegung bzw. Ausführung den wesentlichen Interessen des betreffenden Mitgliedstaats im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung zuwiderlaufen würde. Bevor die zuständige Behörde ein solches Ersuchen ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden sowie – auf Ersuchen eines der betreffenden Mitgliedstaaten – die Kommission.

(3) Die zuständigen Behörden verschiedener Mitgliedstaaten können gemeinsame Aufsichtsmaßnahmen durchführen, wenn dies angebracht ist und im gegenseitigen Einvernehmen geschieht.

(4) Angesichts der Verpflichtung zur Wahrung der Grundsätze der Vertraulichkeit und des Berufs- und Geschäftsgeheimnisses gemäß Artikel 114 Absatz 6 dürfen Informationen, die im Rahmen eines Amtshilfeersuchens ausgetauscht und gemäß diesem Artikel bereitgestellt werden, ausschließlich in Bezug auf die Angelegenheit verwendet werden, für die sie eingeholt wurden.

Artikel 117
Rechtliche Zuständigkeit und Territorialität

(1) Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art, die in den Anwendungsbereich dieser Verordnung fallen, gelten als der rechtlichen Zuständigkeit des Mitgliedstaats unterliegend, in dem sie niedergelassen sind, außer in folgenden Fällen:

a) Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie ihre Dienste erbringen;

b) DNS-Diensteanbieter, Namenregister der Domäne oberster Stufe (TLD), Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, die als der Zuständigkeit des Mitgliedstaats

unterliegend betrachtet werden, in dem sie gemäß Absatz 2 ihre Hauptniederlassung in der Union haben;

c) Einrichtungen der öffentlichen Verwaltung, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, zu dem sie gehören;

d) Luftfahrtunternehmen, die der rechtlichen Zuständigkeit des Mitgliedstaats unterliegen, dessen zuständige Genehmigungsbehörde der Einrichtung gemäß der Verordnung (EG) Nr. 1008/2008 des Europäischen Parlaments und des Rates[83] die Betriebsgenehmigung erteilt hat, oder – falls die Betriebsgenehmigung oder eine gleichwertige Genehmigung nicht gemäß der genannten Verordnung erteilt wurde – die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie gemäß Absatz 2 ihre Hauptniederlassung in der Union haben.

(2) Für die Zwecke dieser Verordnung wird davon ausgegangen, dass als Hauptniederlassung in der Union einer in Absatz 1 Buchstabe b genannten Einrichtung jeweils die Niederlassung in demjenigen Mitgliedstaat betrachtet wird, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden solche Entscheidungen nicht in der Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die meisten Cybersicherheitsmaßnahmen durchgeführt werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Union hat.

(3) Hat eine Einrichtung der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art keine Niederlassung in der Union, bietet aber Dienste innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es wird davon ausgegangen, dass eine solche Einrichtung der Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist. Handelt es sich bei einer solchen Einrichtung um eine Einrichtung im Sinne von Absatz 1 Buchstabe a, so wird davon ausgegangen, dass sie der Zuständigkeit des Mitgliedstaats unterliegt, in dem sie ihre Dienste anbietet. Wurde in der Union kein Vertreter im Sinne dieses Absatzes benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste anbietet, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Verordnung einleiten.

(4) Die Benennung eines Vertreters durch eine in Absatz 1 Buchstabe b genannte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

(5) Mitgliedstaaten, die ein Amtshilfeersuchen zu einer in Absatz 1 Buchstabe b genannten Einrichtung erhalten haben, können innerhalb der Grenzen dieses Ersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die betreffende Einrichtung ergreifen, sofern die Einrichtung in ihrem Hoheitsgebiet Dienste anbietet oder ein Netz- und Informationssystem betreibt.

---

[83] Verordnung (EG) Nr. 1008/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 über gemeinsame Vorschriften für die Durchführung von Luftverkehrsdiensten in der Gemeinschaft (Neufassung) (ABl. L 293 vom 31.10.2008, S. 3, ELI: https://eur-lex.europa.eu/eli/reg/2008/1008/oj/deu).

TITEL VI
SCHLUSSBESTIMMUNGEN

Artikel 118
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss hat zwei Zusammensetzungen. In Bezug auf die Titel II und III wird die Kommission von einem Ausschuss in der ersten Zusammensetzung unterstützt, und in Bezug auf Titel IV wird die Kommission von einem Ausschuss in der zweiten Zusammensetzung unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Artikel 119
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 80 Absatz 2 und Artikel 110 Absatz 5 wird der Kommission auf unbestimmte Zeit ab dem Datum des Inkrafttretens dieser Verordnung übertragen.

(3) Die Befugnisübertragung gemäß Artikel 80 Absatz 2 und Artikel 110 Absatz 5 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 80 Absatz 2 und Artikel 110 Absatz 5 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 120
Bewertung und Überarbeitung

(1) Bis zum [TT.MM.JJJJ] und danach alle fünf Jahre veranlasst die Kommission eine Bewertung, die entsprechend den Leitlinien der Kommission durchgeführt wird.

(2) Im Rahmen der in Absatz 1 genannten Bewertung ist unter anderem Folgendes zu beurteilen:

a) die Leistung der ENISA im Verhältnis zu ihren Zielen, ihrem Mandat, ihrem Auftrag, ihren Aufgaben, ihrer Leitung und ihrem Standort;

b) die Wirksamkeit, die Effizienz und der EU-Mehrwert der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen gemäß Titel II Kapitel II Abschnitt 4 dieser Verordnung;

c) die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III dieser Verordnung im Hinblick auf die Ziele, ein angemessenes Maß an Cybersicherheit für IKT-Produkte, -Dienste und -Prozesse und verwaltete Sicherheitsdienste sowie Einrichtungen in der Union und einen besser funktionierenden Binnenmarkt zu gewährleisten;

d) die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels IV dieser Verordnung im Hinblick auf die Ziele des Rahmens für vertrauenswürdige IKT-Lieferketten.

(3) Im Rahmen der in Absatz 1 Buchstabe a genannten Bewertung wird insbesondere geprüft, ob das Mandat der ENISA möglicherweise geändert werden muss und welche finanziellen Auswirkungen eine solche Änderung hätte.

(4) Bei jeder zweiten Bewertung gemäß Absatz 1 Buchstabe a bewertet die Kommission die von der ENISA erzielten Ergebnisse im Hinblick auf ihre Ziele, ihr Mandat, ihren Auftrag, ihre Leitung und ihre Aufgaben, einschließlich einer Bewertung der Frage, ob die Weiterführung der ENISA im Hinblick auf diese Ziele, dieses Mandat, diesen Auftrag, diese Leitung und diese Aufgaben noch gerechtfertigt ist.

(5) Die Kommission legt die Ergebnisse der Bewertung dem Europäischen Parlament, dem Rat und dem Verwaltungsrat vor. Die Ergebnisse der Bewertung werden veröffentlicht.

Artikel 121
Aufhebung und Weiterführung der Tätigkeiten

(1) Die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates wird mit Wirkung vom TT.MM.JJJJ aufgehoben.

(2) Verweise auf die Verordnung (EU) 2019/881, die ENISA und europäische Systeme für die Cybersicherheitszertifizierung gemäß der genannten Verordnung gelten als Verweise auf die vorliegende Verordnung und sind nach der Entsprechungstabelle in Anhang III dieser Verordnung zu lesen.

(3) Die der vorliegenden Verordnung unterliegende ENISA führt in Bezug auf das Eigentum und alle Abkommen, rechtlichen Verpflichtungen, Beschäftigungsverträge, finanziellen Verpflichtungen und Verbindlichkeiten die Maßnahmen und Tätigkeiten der durch die Verordnung (EU) 2019/881 errichteten ENISA weiter. Alle vom Verwaltungsrat und vom Exekutivrat gemäß der Verordnung (EU) 2019/881

getroffenen Entscheidungen bleiben gültig, sofern sie der vorliegenden Verordnung nicht zuwiderlaufen.

(4) Der nach Artikel 15 Absatz 1 Buchstabe n der Verordnung (EU) 2019/881 ernannte Exekutivdirektor bleibt im Amt und übernimmt die Aufgaben und Zuständigkeiten des Exekutivdirektors nach Artikel 32 der vorliegenden Verordnung für die restliche Dauer seiner Amtszeit. Seine sonstigen Vertragsbedingungen bleiben unverändert.

(5) Die möglichen Systeme, deren Ausarbeitung gemäß Artikel 49 der Verordnung (EU) 2019/881 in Auftrag gegeben wurde, gelten als gemäß den entsprechenden Bestimmungen der vorliegenden Verordnung in Auftrag gegeben. Die Bestimmungen des Titels III der vorliegenden Verordnung gelten für diese möglichen Systeme entsprechend.

(6) Die nach Artikel 14 der Verordnung (EU) 2019/881 von der Kommission ernannten Mitglieder und stellvertretenden Mitglieder des Verwaltungsrats bleiben im Amt und üben die Funktionen des Verwaltungsrats nach Artikel 27 der vorliegenden Verordnung für die restliche Dauer ihrer Amtszeit aus. Die nach Artikel 14 der Verordnung (EU) 2019/881 durch die Mitgliedstaaten ernannten Mitglieder des Verwaltungsrats bleiben im Amt und üben die Funktionen des Verwaltungsrats nach Artikel 27 der vorliegenden Verordnung aus, sofern sie Funktionen gemäß Artikel 24 Absatz 3 der vorliegenden Verordnung innehaben.

Artikel 122
Inkrafttreten

Diese Verordnung tritt am [...] Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Straßburg am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident/Die Präsidentin*

FINANZ- UND DIGITALBOGEN ZU RECHTSAKTEN

1. RAHMEN DES VORSCHLAGS/DER INITIATIVE

1.1. Bezeichnung des Vorschlags/der Initiative

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)

(Text von Bedeutung für den EWR)

Kurztitel: Cybersicherheitsverordnung 2 (CSA2)

und

Vorschlag für eine Richtlinie zur Änderung der Richtlinie (EU) 2022/2555 im Hinblick auf Vereinfachungsmaßnahmen und die Angleichung an den [Vorschlag für die Cybersicherheitsverordnung 2]

1.2. Politikbereich(e)

Politikbereich: 09 – Kommunikationsnetze, Inhalte und Technologien

Tätigkeitsbereich: 09 02 – Digitaler Binnenmarkt

1.3. Ziel(e)

1.3.1. Allgemeine(s) Ziel(e)

Mit dem Tätigwerden soll im Wesentlichen Folgendes erreicht werden:

1. ***Verbesserung der Cybersicherheitskapazitäten und der Resilienz***

Beitrag zur Stärkung der Governance der Union im Bereich Cybersicherheit sowie Beitrag dazu, dass die einschlägigen Organe, Behörden und anderen Interessenträger besser darauf vorbereitet sind, Cybersicherheitsbedrohungen koordiniert und wirksam zu verhindern, zu erkennen und darauf zu reagieren.

2. ***Verhinderung der Fragmentierung im gesamten Binnenmarkt***

Unterstützung der Entwicklung, Umsetzung und Einführung gemeinsamer Cybersicherheitsinstrumente der Union, wie z. B. Zertifizierungssysteme, und Bereitstellung harmonisierter Rahmen zum Aufbau von Vertrauen und Interoperabilität zwischen den Mitgliedstaaten.

Diese allgemeinen Ziele sind die Antwort auf die wichtigsten Herausforderungen, die im Rahmen der Problemstellung gemäß der Folgenabschätzung zur vorgeschlagenen Initiative ermittelt wurden. Sie spiegeln das übergeordnete politische Ziel wider, die Governance im Bereich der Cybersicherheit in der Union zu stärken und die Entwicklung eines sicheren, widerstandsfähigen und wettbewerbsfähigen digitalen Binnenmarkts zu unterstützen.

1.3.2. Einzelziel(e)

Behebung der Diskrepanz zwischen dem politischen Rahmen der EU für die Cybersicherheit und den Bedürfnissen der Interessenträger:

Einzelziel Nr. 1: Schaffung der Kapazitäten für die wirksame Umsetzung der Cybersicherheitspolitik der Union und für eine kontinuierliche operative

Zusammenarbeit, die eine strukturiertere Zusammenarbeit zwischen den Mitgliedstaaten ermöglicht.

Einzelziel Nr. 2: Entwicklung und Umsetzung von Mitteln und Mechanismen zur wirksamen Unterstützung und Deckung des Bedarfs der Mitgliedstaaten, der Industrie und anderer Interessenträger.

Umgang mit der begrenzten Verbreitung und Wirksamkeit des europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF):

Einzelziel Nr. 3: Schaffung der Voraussetzungen für eine schnellere Bereitstellung von Systemen für die Cybersicherheitszertifizierung auf der Grundlage des Marktbedarfs, indem der Umfang des ECCF ausgeweitet wird, eine wirksame Systempflege und flexible Verfahren sichergestellt werden und die Transparenz erhöht wird.

Verringerung der Fragmentierung der Rechtsvorschriften und der Komplexität horizontaler und sektoraler Regelungen:

Einzelziel Nr. 4: Schaffung von Mechanismen und Bedingungen, um die Einhaltung der Anforderungen an die Cybersicherheit zu erleichtern und so ihre Umsetzung kohärenter und wirksamer zu gestalten.

Bewältigung von Cybersicherheitsrisiken in den Lieferketten:

Einzelziel Nr. 5: Verringerung der Risiken bei kritischen IKT-Lieferketten von Einrichtungen, die in Ländern, für die Cybersicherheitsbedenken bestehen, niedergelassen sind oder von Einrichtungen in diesen Drittländern kontrolliert werden (Hochrisikoanbieter), und Verringerung kritischer Abhängigkeiten durch die Entwicklung eines kohärenten und wirksamen Rahmens auf EU-Ebene zur Bewältigung von Risiken für die Sicherheit von IKT-Lieferketten.

1.3.3. Erwartete Ergebnisse und Auswirkungen

Bitte geben Sie an, wie sich der Vorschlag/die Initiative auf die Begünstigten/Zielgruppen auswirken sollte.

Folgende Ergebnisse werden erwartet:

1. Funktionale Reform der ENISA

2. Reform des ECCF – Ausweitung des Anwendungsbereichs, neues Verfahren und überarbeitete Governance

3. Weitere Vereinfachung der Einhaltung des einschlägigen Rechtsrahmens der Union für die Cybersicherheit

4. Umfassender horizontaler Rahmen, um den Cybersicherheitsrisiken in den IKT-Lieferketten zu begegnen

Gesamtauswirkungen:

Der Vorschlag wird enorme Auswirkungen auf die Cybersicherheit in der Union haben, da damit eine Reihe von Bereichen in Angriff genommen werden, darunter die erforderliche Stärkung der Agentur der Europäischen Union für Cybersicherheit, die Unterstützung für die Umsetzung des EU-Rechts gestärkt wird, Reformen für eine reibungslose Umsetzung des europäischen Zertifizierungsrahmens einführt werden, das gemeinsame Verständnis der Union von Cyberbedrohungen unterstützt und die Minderung von Cybersicherheitsrisiken entsprechend der geopolitischen Realität angegangen wird. Die Umsetzung der vorgeschlagenen Bestimmungen wird

ein hohes Maß an Effizienz und Kohärenz gewährleisten und einen übermäßigen Regelungsaufwand vermeiden. Das Paket ist so konzipiert, dass es den Herausforderungen bei der Umsetzung standhält und die langfristige politische Kohärenz im gesamten digitalen Ökosystem und Cybersicherheitsökosystem unterstützt. Es trägt zur Verbesserung der Klarheit, zur Beseitigung von Ineffizienzen und zur Angleichung der Verfahren in allen Rechtsrahmen bei und unterstützt gleichzeitig die Verwirklichung eines hohen Cybersicherheitsniveaus in der gesamten EU. Als eines der wichtigsten vorrangigen Ziele der EU-Kommission werden die geplanten Vereinfachungsbemühungen erhebliche wirtschaftliche Vorteile für Unternehmen, einschließlich KMU, in Höhe von mehr als 14,63 Mrd. EUR und für Behörden in Höhe von 7,5 Mio. EUR bringen.

Zu den spezifischen Ergebnissen gehört Folgendes:

– stärkere Sensibilisierung und bessere operative Koordinierung, was zu erheblichen Kosteneinsparungen im Zusammenhang mit der schnelleren Erkennung von Sicherheitsvorfällen und der schnelleren Reaktion darauf für Unternehmen, Behörden sowie Bürgerinnen und Bürger führen könnte;

– klare Festlegung des Aufgabenbereichs und der Zuständigkeiten der ENISA bei gleichzeitiger Gewährleistung der notwendigen Priorisierung ihrer Hauptaufgaben;

– Gewährleistung, dass die Interessenträger angemessene Unterstützung bei der Umsetzung der Politik, operativen Tätigkeiten und der Gesamtkoordinierung erhalten;

– Unterstützung des gemeinsamen Lageerfassung der Union;

– Verbesserung der Zusammenarbeit mit dem EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission, Europol, dem CERT-EU und anderen einschlägigen Einrichtungen der Union, um Ablagen verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen zu entwickeln;

– Unterstützung der Bemühungen zur Eindämmung von Ransomware-Angriffen;

– bessere Koordinierung mit dem Privatsektor in Fragen der Cybersicherheit;

– zeitnahe Verbreitung von Informationen mithilfe von Frühwarnungen in Bezug auf einen erheblichen Sicherheitsvorfall oder Sicherheitsvorfall großen Ausmaßes oder eine grenzübergreifende Cyberbedrohung in Bezug auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren;

– Förderung wirksamer Synergien mit anderen Einrichtungen und Agenturen der EU;

– Senkung der Preise für die Zertifizierung von Kompetenzen, unter anderem durch die Erhöhung des Angebots auf dem Markt durch die Einführung der Systeme europäischer Einzelbescheinigungen von Kompetenzen;

– Unterstützung bei der Schließung der Kompetenzlücke in Europa durch Einzelbescheinigungen von Cybersicherheitskompetenzen und Unterstützung der Mitgliedstaaten und der Industrie beim Ausbau ihrer Arbeitskräftebasis;

– Beseitigung der mangelnden Klarheit des ECCF-Rahmens und seiner begrenzten Wirkung, Ausweitung seines Anwendungsbereichs und Verbesserung seines Governance-Modells;

– Verbesserung des Ansehens angenommener Programme durch die Einrichtung einer Systempflegeinfrastruktur und die Einführung eines zeitnahen und transparenten Entwicklungsprozesses;

– Einführung eines Gebührenmechanismus in Bezug auf die Kosten für die Entwicklung und Pflege der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, die Bearbeitung von Anträgen und die Erteilung von Befugnissen an Anbieter sowie für die Pflege der im Rahmen des ECCF angenommenen Systeme, was zur Finanzstabilität der Agentur beitragen und Einsparungen im Rahmen des EU-Haushalts bewirken wird;

– Angleichung der europäischen Zertifizierungssysteme an den bestehenden Rechtsrahmen und damit bessere Unterstützung der Umsetzungsbemühungen und Unterstützung des Bedarfs der Unternehmen in Bezug auf die Einhaltung der Vorschriften;

– Ermöglichung der Annahme derzeit blockierter Systeme;

– Förderung der Wettbewerbsfähigkeit europäischer Unternehmen durch Förderung der Angleichung internationaler und europäischer Normen;

– Begrenzung der Fragmentierung bei Cybersicherheitsmaßnahmen und -anforderungen;

– Gewährleistung von Rechtsklarheit und erhebliche Verringerung des Verwaltungsaufwands, ohne dass dies zu erheblicher Rechtsunsicherheit bei den Interessenträgern führt, die sich derzeit an die kürzlich angenommenen Rechtsrahmen anpassen;

– Erleichterung der Einhaltung der Vorschriften durch NIS-2-Einrichtungen, was auch zu einer insgesamt höheren Einhaltungsquote und zu sinnvolleren Cybersicherheitsmaßnahmen beitragen und gleichzeitig das Aufsichtsverfahren aufseiten der Behörden effizienter machen würde.

Sonstiges:

– Angesichts der verbesserten Wettbewerbsfähigkeit auf dem EU-Cybersicherheitsmarkt sowie der geringeren Kosten und des geringeren Verwaltungsaufwands hätte die Initiative für KMU zahlreiche positive Auswirkungen:

1. *Positive Rolle für KMU, die aufgrund einer gestärkten Rolle der ENISA und der von der Agentur bereitgestellten technischen Leitlinien von einer erhöhten Cyberresilienz profitieren würden.*

2. *KMU als befugte Anbieter, die zur Ausstellung von Bescheinigungen im Rahmen des Systems europäischer Einzelbescheinigungen von Kompetenzen befugt sind, werden an Sichtbarkeit, Ansehen und Kunden gewinnen. Darüber hinaus werden die europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen KMU dabei unterstützen, Bewerber mit den richtigen Kompetenzen zu finden.*

3. *Gut funktionierende europäische Zertifizierungssysteme können KMU die Auswahl vertrauenswürdiger IKT-Technologien erleichtern und dazu beitragen, ihre Cyberresilienz insgesamt zu verbessern.*

4. *Als DNS-Anbieter werden KMU aufgrund der Ausnahmen für DNS-Anbieter von deren Anwendungsbereich von Maßnahmen im Zusammenhang mit der Umsetzung der NIS-2-Richtlinie profitieren.*

5. *KMU würden von den Präzisierungen des Anwendungsbereichs profitieren, die die Anwendung der Verpflichtungen auf bestimmte Einrichtungen in einigen in der NIS-2-Richtlinie aufgeführten Sektoren beschränken würden.*

6. *Bei Maßnahmen für die Sicherheit der IKT-Lieferketten würden KMU im Allgemeinen vom Einsatz vertrauenswürdiger Technologien profitieren. Als Anbieter, die in den Wirtschaftszweigen tätig sind, die Beschränkungen unterliegen, wären sie im Vergleich zu größeren Unternehmen stärker von Substitutionen und Transaktionskosten betroffen. KMU als vertrauenswürdige Anbieter werden jedoch neue Marktchancen zugutekommen.*

– Für keines der Ziele wird mit signifikanten ökologischen Auswirkungen gerechnet.

– Für den EU-Haushalt sind Effizienzgewinne infolge einer verstärkten Zusammenarbeit und Koordinierung der Tätigkeiten zwischen den Organen, Einrichtungen und sonstigen Stellen der EU zu erwarten. Langfristig werden Einsparungen durch die Einführung von Gebührenmechanismen erwartet.

1.3.4. Leistungsindikatoren

Bitte geben Sie an, anhand welcher Indikatoren die Fortschritte und Ergebnisse verfolgt werden sollen.

Ziel: Schaffung der Kapazitäten für die wirksame Umsetzung der EU-Cybersicherheitspolitik und für eine regelmäßige/kontinuierliche operative Zusammenarbeit, die eine strukturiertere Zusammenarbeit zwischen den Mitgliedstaaten ermöglicht.

– Anzahl der relevanten Beiträge der ENISA zur Umsetzung der politischen Maßnahmen und Gesetzgebungsinitiativen der EU und der Mitgliedstaaten

– positive Rückmeldungen der Interessenträger zu den relevanten Beiträgen der ENISA

– Steigerung um 25 % gegenüber dem Ausgangswert von 2023, wie im jährlichen Tätigkeitsbericht der ENISA (für die Anzahl der relevanten Beiträge) und in der jährlichen Zufriedenheitsumfrage der ENISA (für die positiven Rückmeldungen) angegeben

– Nutzungsstatistiken der EU-Schwachstellendatenbank

– Anstieg der Zahl der Nutzer um 25 % gegenüber 2025

– Verfügbarkeit, Sicherheit und Funktionsweise der Plattform im Rahmen der Cyberresilienzverordnung

– Verringerung der Ausfallzeiten der Plattform um 25 % und der Zahl der Sicherheitsvorfälle im Vergleich zu Statistiken über Ausfallzeiten und Sicherheitsvorfälle auf der Plattform aus dem Jahr 2025

Ziel: Entwicklung und Einsatz von Mitteln und Mechanismen zur wirksamen Unterstützung und Deckung des Bedarfs der Mitgliedstaaten, der Industrie und anderer Interessenträger.

– Anzahl der von der ENISA unterstützten Interessenträger und Qualität der bereitgestellten Unterstützung

– Anzahl der Maßnahmen zur Unterstützung der Interessenträger

– Steigerung der Anzahl der unterstützten Interessenträger um 10 % und der Zufriedenheit der unterstützten Interessenträger um 10 % gegenüber 2025

Ziel: Schaffung der Voraussetzungen für eine schnellere Bereitstellung von Systemen für die Cybersicherheitszertifizierung auf der Grundlage des Marktbedarfs, indem der Umfang des ECCF ausgeweitet wird, eine wirksame Systempflege und flexible Verfahren sichergestellt werden und die Transparenz erhöht wird.

– Anzahl der angenommenen Systeme

– Verkürzung der Zeit für die Entwicklung eines Systems um 50 % gegenüber 2025

– Zahl der jährlich ausgestellten gültigen Zertifikate

– Steigerung um 25 % gegenüber dem Ausgangswert von 2025

– positive Rückmeldungen der Interessenträger in Bezug auf ihre Beteiligung an der Systementwicklung und Transparenz des ECCF

– Steigerung um 25 % gegenüber dem Ausgangswert in der jährlichen Zufriedenheitsumfrage der ENISA im Vergleich zu 2027

Ziel: Einrichtung von Mechanismen und Bedingungen, um die Einhaltung der Anforderungen an die Cybersicherheit zu erleichtern und so ihre Umsetzung kohärenter und wirksamer zu gestalten.

– Prozentualer Anteil der KMU-Kosten für die Einhaltung der NIS-2- und Cybersicherheitsvorschriften an den gesamten Befolgungskosten

– > 70 % KMU melden eine Verringerung der Befolgungskosten im Bereich der Cybersicherheit gegenüber 2025.

– Zahl der Ransomware-Angriffe und Schadenshöhe in EUR

– Verringerung der Zahl der Ransomware-Angriffe um > 1 % gegenüber 2027

– Prozentsatz der grenzübergreifenden Sicherheitsvorfälle, bei denen oder nach denen die Behörden der Mitgliedstaaten Amtshilfemechanismen in Anspruch genommen haben

– Erhöhung des Anteils der Fälle, in denen die Amtshilfe in Anspruch genommen wurde, um > 20 Prozentpunkte gegenüber 2025

Ziel: Verringerung kritischer Abhängigkeiten durch die Entwicklung eines kohärenten und wirksamen Rahmens auf EU-Ebene zur Bewältigung von Risiken für die Sicherheit von IKT-Lieferketten.

– Anzahl der ergriffenen Maßnahmen

– Steigerung der Zahl der angenommenen Maßnahmen und der wichtigen Assets um 25 % gegenüber dem Datum der Annahme + 6 Monate

– Verringerung der Abhängigkeit von Hochrisikoanbietern bei wichtigen IKT-Assets um 25 % gegenüber 2025

1.4. Der Vorschlag/Die Initiative betrifft

☒ eine neue Maßnahme *(Titel IV Lieferkette, Titel V Vereinfachung)*

☐ eine neue Maßnahme im Anschluss an ein Pilotprojekt/eine vorbereitende Maßnahme[84]

☒ die Verlängerung einer bestehenden Maßnahme *(Titel II Mandat der ENISA und Titel III Zertifizierung)*

☐ die Zusammenführung mehrerer Maßnahmen oder die Neuausrichtung mindestens einer Maßnahme

1.5. Begründung des Vorschlags/der Initiative

1.5.1. Kurz- oder langfristig zu deckender Bedarf, einschließlich einer detaillierten Zeitleiste für die Durchführung der Initiative

Im Juli 2024 forderte die Präsidentin der Europäischen Kommission Ursula von der Leyen in ihren politischen Leitlinien[85] eine Vereinfachung, Konsolidierung und Kodifizierung der EU-Rechtsvorschriften, damit Überschneidungen und Widersprüchlichkeiten unter Aufrechterhaltung hoher Standards beseitigt werden. Im Mandatsschreiben an Exekutiv-Vizepräsidentin Virkkunen[86] wird insbesondere auf die Verbesserung des Verfahrens zur Annahme europäischer Systeme für die Cybersicherheitszertifizierung und die Notwendigkeit hingewiesen, unsere Wirtschaft, Bürgerinnen und Bürger sowie öffentlichen Verwaltungen vor internen und externen Bedrohungen zu schützen. Darüber hinaus wird im Niinistö-Bericht[87] von 2024 gefordert, das Risiko unerwünschter Abhängigkeiten in Lieferketten bei kritischen Technologien zu verringern. Zentrale Aspekte der von der EU-Präsidentin in Auftrag gegebenen Draghi[88]- und Letta[89]-Berichte befassten sich mit der Notwendigkeit, den Binnenmarkt durch Vereinfachung wettbewerbsfähig zu halten und ein Höchstmaß an Sicherheit und strategischer Autonomie zu gewährleisten. Vor diesem Hintergrund ist die Überarbeitung des CSA ein Eckpfeiler der Arbeit der Kommission im Bereich der Sicherheit und stellt die Umsetzung einer ehrgeizigen Überarbeitung des europäischen Regulierungsökosystems für die Cybersicherheit dar. Mit dem CSA2-Vorschlag werden Mechanismen zur Bewältigung von Cybersicherheitsrisiken in den Lieferketten und Mechanismen zur Verringerung der Fragmentierung der Rechtsvorschriften und der Komplexität horizontaler und sektoraler Regelungen eingeführt. Es wird erwartet, dass die ENISA auch ein Instrument sein wird, das durch die Integration einer zentralen Anlaufstelle zu einer größeren Vereinfachung der Berichtspflichten führen wird.

Darüber hinaus muss das Mandat der ENISA angesichts der zahlreichen sektorspezifischen Bestimmungen, die nach der Annahme des CSA im Jahr 2019 eingeführt wurden, sowie der sich rasch wandelnden Bedrohungslage im Bereich der Cybersicherheit überprüft werden, um gezieltere und neue Aufgaben festzulegen und so die Bemühungen der Mitgliedstaaten, der EU-Organe und anderer Interessenträger um die Gewährleistung eines sicheren Cyberraums in der Europäischen Union

84 Im Sinne des Artikels 58 Absatz 2 Buchstabe a oder b der Haushaltsordnung.
85 Politische Leitlinien 2024.
86 Mandatsschreiben an Exekutiv-Vizepräsidentin Virkkunen.
87 Bericht von Sauli Niinistö.
88 Draghi-Bericht über die Wettbewerbsfähigkeit der EU.
89 Enrico Letta – *Much more than a market* (April 2024).

wirksam und effizient zu unterstützen. Durch die Stärkung des Europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF) wird mit dem Vorschlag sichergestellt, dass die EU über ein schlankes, modernes und anpassungsfähiges Zertifizierungssystem verfügt, das den Maßnahmen in den Lieferketten und der raschen Umsetzung der Cyberresilienzverordnung dient. Zusammenfassend lässt sich sagen, dass der vorgeschlagene Umfang des Mandats abgegrenzt wird, indem die Bereiche gestärkt werden, in denen die Agentur einen eindeutigen Mehrwert bewiesen hat, und indem neue Bereiche hinzugefügt werden, in denen angesichts der neuen politischen Prioritäten und Instrumente sowie zur Stärkung des ECCF Unterstützung benötigt wird.

Die Überarbeitung des CSA ist daher als ein wichtiger Schritt für die Cyberabwehr der EU und die allgemeine Sicherheit, Abwehrbereitschaft und Resilienz der Europäischen Union konzipiert.

1.5.2. Mehrwert aufgrund des Tätigwerdens der EU (kann sich aus unterschiedlichen Faktoren ergeben, z. B. Vorteile durch Koordinierung, Rechtssicherheit, größere Wirksamkeit oder Komplementarität). Für die Zwecke dieses Abschnitts bezeichnet der Ausdruck „Mehrwert aufgrund des Tätigwerdens der EU“ den Wert, der sich aus dem Tätigwerden der EU ergibt und den Wert ergänzt, der andernfalls allein von den Mitgliedstaaten geschaffen worden wäre.

Der Rechtsakt zur Cybersicherheit wurde 2019 auf der Rechtsgrundlage von Artikel 114 AEUV angenommen, der den Gesetzgeber der EU ermächtigt, Maßnahmen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten zu erlassen, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben.

Der überarbeitete Vorschlag für eine Cybersicherheitsverordnung soll die Rechtsvorschriften zur Cybersicherheit auf EU-Ebene zu straffen und den geltenden Rechtsakt zur Cybersicherheit, der seit 2019 in Kraft ist (CSA1), ergänzen und überarbeiten. Die Ziele des CSA1 im Hinblick darauf, der Agentur der Europäischen Union für Cybersicherheit ein ständiges Mandat zu erteilen, um das hohe gemeinsame Cybersicherheitsniveau in der gesamten EU zu unterstützen und eine Fragmentierung des Binnenmarkts in Bezug auf Systeme für die Cybersicherheitszertifizierung zu vermeiden, werden im Rahmen der eingeleiteten Überarbeitung beibehalten. Diese Ziele, die bereits 2017 im Rahmen des Vorschlags für einen Rechtsakt zur Cybersicherheit ordnungsgemäß analysiert wurden, können von den Mitgliedstaaten nicht ausreichend verwirklicht werden, sondern nur auf Ebene der Europäischen Union im Einklang mit Artikel 5 des Vertrags über die Europäische Union.

Der Vorschlag für die Überarbeitung des CSA konzentriert sich eindeutig auf die Straffung, Priorisierung und Kodifizierung von Aufgaben in allen Rechtsvorschriften im Cyberbereich, die nur auf EU-Ebene erreicht werden könnten, und es gibt derzeit keine entsprechende Initiative. Der neue Vorschlag stärkt die Sicherheit der Lieferketten und des Cybersicherheitssektors in der EU weiter und verbessert die Abwehrbereitschaft und Resilienz der Mitgliedstaaten und der Industrie. Abhängigkeiten von Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder von einer Einrichtung aus diesem Drittland kontrolliert werden (Hochrisikoanbieter), betreffen Einrichtungen in der gesamten Union, und schwerwiegende Cybersicherheitsvorfälle in den Lieferketten breiten sich häufig über nationale Grenzen hinweg aus. Es ist

unwahrscheinlich, dass das Problem allein auf nationaler Ebene wirksam angegangen werden kann.

Die der ENISA neu übertragenen Aufgaben sind von entscheidender Bedeutung, um ein hohes Maß an Cybersicherheit in der gesamten EU zu erreichen. Obwohl die Agentur mit anderen Sicherheitseinrichtungen der EU wie Europol sowie dem Europäischen Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit (ECCC), das für die Finanzierung der Umsetzung zuständig ist, zusammenarbeitet, sind der Auftrag und die Aufgaben der Agentur einzigartig, und derzeit gibt es keine andere Stelle, die diese Art von Zuständigkeiten wahrnimmt. Im Cyber-Ökosystem der EU arbeiten alle beteiligten Einrichtungen in enger Synergie und im Rahmen klarer Mandate. Daher werden mit dem CSA2-Vorschlag nur die Bereiche gestärkt, in denen ein eindeutiger Mehrwert besteht, um sicherzustellen, dass es keine Unklarheiten in Bezug auf Doppelarbeit gibt, und zwar nicht nur im Hinblick auf den Inhalt, sondern auch in Bezug auf die Finanzierung mit anderen Stellen innerhalb des Cyber-Ökosystems.

Im Einzelnen

Das Mandat der ENISA wurde durch nachfolgende Rechtsvorschriften erweitert, ohne dass ihre grundlegenden Zuständigkeiten und ihre Ressourcen angepasst wurden. Dies hat Überschneidungen und Ineffizienzen hervorgebracht und dazu geführt, dass die Kernaufgaben zur Unterstützung der Mitgliedstaaten nicht ausreichend priorisiert wurden.

Mehrere Mitgliedstaaten haben ihre eigenen nationalen Systeme für die Cybersicherheitszertifizierung eingeführt, die sich in Umfang und Konformitätsbewertungsverfahren erheblich voneinander unterscheiden. Dies führt zu einer Marktfragmentierung und doppelten Belastungen für Betreiber und KMU, die eine einmalige Zertifizierung anstreben und in der gesamten EU tätig sind. Der ECCF wurde mit dem CSA eingerichtet, um der Marktfragmentierung entgegenzuwirken, aber die Umsetzung verlief langsam und uneinheitlich.

Ebenso sind in mehreren horizontalen und sektorspezifischen Rechtsakten Cybersicherheitsmaßnahmen mit unterschiedlichen Zwecken und Zielen festgelegt, was auch zu Unterschieden bei der Konformitätsprüfung und den Aufsichtsansätzen der Mitgliedstaaten führt. Infolgedessen sind Unternehmen, insbesondere KMU oder Unternehmen, die in mehreren Mitgliedstaaten tätig sind, mit zusätzlichem Befolgungsaufwand konfrontiert, was sich negativ auf ihre Wettbewerbsfähigkeit auswirkt.

Verschiedene Ansätze für die Sicherheit der IKT-Lieferketten und unterschiedliche Maßnahmen der Mitgliedstaaten führen zu einer Marktfragmentierung und unterschiedlichen Einhaltungsanforderungen an Einrichtungen. Insbesondere würde angesichts des grenzübergreifenden Charakters der IKT-Lieferketten eine Fragmentierung der Einhaltungsanforderungen im Binnenmarkt die Rechtssicherheit für Einrichtungen untergraben. Unterschiedliche nationale Rahmen für die Beschränkung von Hochrisikoanbietern bergen die Gefahr, dass Hindernisse für den grenzüberschreitenden Waren- und Dienstleistungsverkehr im Binnenmarkt entstehen. Da die IKT-Lieferketten kritische Einrichtungen und Infrastrukturen umfassen können, unabhängig davon, wo diese Anbieter niedergelassen sind, führen Fragmentierung und Lücken bei den Cybersicherheitsmaßnahmen zu zusätzlichen Sicherheitsrisiken für diese Einrichtungen.

Darüber hinaus enthalten die Vorschläge für die Programme des mehrjährigen Finanzrahmens (MFR) eine horizontale Bestimmung, die den Ausschluss von Hochrisikoanbietern vorschreibt, die nach EU-Recht ermittelt wurden, um die Integrität des EU-Haushalts zu schützen und sicherzustellen, dass die Ausgaben der Union nicht im Widerspruch zu wesentlichen Sicherheitsinteressen der Union stehen. Der CSA-Rahmen für Lieferketten wäre der Mechanismus, der diese Ermittlung im Bereich der IKT-Lieferketten ermöglicht und daher nur auf EU-Ebene durchgeführt werden kann.

Cyberangriffe haben grundsätzlich einen grenzübergreifenden Charakter, insbesondere unter Berücksichtigung von Spillover-Effekten, die von einer zunächst allein betroffenen Eingangsstelle ausgehen könnten. Die Bedrohungen und Risiken im Bereich der Cybersicherheit haben Auswirkungen auf die gesamte Europäische Union, weshalb ein kollektives Lagebild das Cybersicherheitsniveau der Einrichtungen in der Europäischen Union erheblich verbessern könnte. Die Vorschläge im Rahmen des überarbeiteten Mandats der ENISA befassen sich mit diesem Thema, um die Cyberresilienz der EU deutlich zu erhöhen.

Schließlich ist ein Tätigwerden der EU unerlässlich, da Cybersicherheitsbedrohungen und die damit verbundenen Herausforderungen nicht an den Grenzen der Mitgliedstaaten haltmachen. Fragmentierte nationale Lösungen haben sich als unzureichend erwiesen, um Vertrauen und Koordinierung im gesamten Markt zu erreichen. Ein überarbeiteter EU-Rechtsrahmen ist erforderlich, um Hindernisse zu beseitigen, eine einheitliche Umsetzung zu gewährleisten und die Mitgliedstaaten in einem immer komplexeren Regelungs- und Bedrohungsumfeld zu unterstützen.

1.5.3. Aus früheren ähnlichen Maßnahmen gewonnene Erkenntnisse

Die ENISA wurde im Jahr 2004 mit einem befristeten Mandat gegründet. Im Jahr 2019 trat der Rechtsakt zur Cybersicherheit in Kraft, mit dem der ENISA ein ständiges Mandat erteilt und das Ziel übertragen wurde, zum Zentrum für Cyberkompetenz in Europa zu werden. Die ENISA ist heute eine anerkannte Marke und ein vertrauenswürdiger Partner unter den Interessenträgern in der EU. Die Kompetenzen der Agentur wurden im Laufe von 25 Jahren schrittweise aufgebaut, um dem sich wandelnden Cyber-Ökosystem Rechnung zu tragen.

Gemäß Artikel 67 des CSA bewertet die Kommission die Wirkung, Wirksamkeit und Effizienz der ENISA und ihrer Arbeitsmethoden und prüft, ob Änderungen erforderliche sind und welche finanziellen Auswirkungen solche Änderungen hätten. Zudem werden die Wirkung, Wirksamkeit und Effizienz der Bestimmungen in Bezug auf den europäischen Rahmen für Cybersicherheitszertifizierung bewertet.

Gemäß den Bestimmungen hat die Kommission eine Bewertung der Agentur und des europäischen Rahmens für die Cybersicherheitszertifizierung durchgeführt, was eine öffentliche Konsultation und eine unabhängige Studie umfasste. Im Einklang mit den Verfahren für eine bessere Rechtsetzung hat die Kommission auch eine öffentliche Konsultation speziell zur Überarbeitung des CSA sowie eine Aufforderung zur Stellungnahme eingeleitet, um Daten von den Interessengruppen zu sammeln. Die Bewertung kam zu dem Schluss, dass die ENISA ihren Auftrag erfüllt hat, indem sie fast alle geplanten Outputs erbracht hat. Die Ziele der Agentur sind heute nach wie vor relevant, wobei die Ergebnisse von Interessenträgern insbesondere in schwierigen Zeiten wie der COVID-19-Pandemie und dem russischen Angriffskrieg gegen die Ukraine anerkannt wurden. Trotz der allgemein positiven Rückmeldungen der Interessenträger zu den Ergebnissen der ENISA zeigte sich auch, dass

erheblicher Verbesserungsbedarf besteht, um den Erwartungen der Interessenträger durchweg gerecht zu werden.

Die gewonnenen Erkenntnisse haben gezeigt, dass zur Steigerung der Effizienz der ENISA ein stärkerer strategischer Fokus, die Priorisierung von Aufgaben und die Stärkung ihrer Fähigkeit, zeitnah Einblicke in neu aufkommende Bedrohungen zu geben und strategische Instrumente zu ihrer Bewältigung bereitzustellen, erforderlich sind. Darüber hinaus könnte die ENISA, wie von einer Reihe von Interessenträgern angemerkt, strukturiertere und transparentere Methoden für die Zusammenarbeit mit privaten Einrichtungen einführen, wobei der Schwerpunkt auf der Unterstützung von KMU liegen sollte. In allen externen Konsultationen wurde betont, wie wichtig es ist, die finanziellen, personellen und operativen Kapazitäten der ENISA aufzustocken, damit sie den wachsenden Anforderungen der Cybersicherheitslandschaft der EU gerecht werden kann. In ihrem Bewertungsbericht im Anschluss an die Studie stellten die Kommissionsdienststellen den eindeutigen Bedarf an zukunftssicheren Rechtsvorschriften, die an die komplexe und sich rasch entwickelnde Cyberbedrohungslandschaft angepasst werden können, bzw. die Notwendigkeit fest, die Agentur mit den erforderlichen Ressourcen zu stärken, um die Unterstützung für ein Höchstmaß an Cybersicherheit in Europa sicherzustellen. Auf der Grundlage der gesammelten Daten und der Erfahrungen mit der Umsetzung des CSA wurde der Schluss gezogen, dass die Koordinierung mit anderen Stellen gestrafft werden sollte und dass der Schwerpunkt auf die Unterstützung bei der Umsetzung des EU-Rechts durch die ENISA und auf die auf Ersuchen bereitgestellte Unterstützung der Kommission bei der Ausarbeitung von Rechtsvorschriften im Bereich der Cybersicherheit gelegt werden sollte. In dem Vorschlag werden Synergien mit den geopolitischen Prioritäten der Kommission geprüft, um Risiken wie die zunehmende Abhängigkeit von Einrichtungen anzugehen, die in Ländern, für die Cybersicherheitsbedenken bestehen, in Europa niedergelassen sind und von diesen kontrolliert werden (Hochrisikoanbieter). Als Kompetenzzentrum dient die ENISA derzeit auch ein wichtiges Informationsarchiv, das für den Aufbau eines gemeinsamen Verständnisses der Bedrohungen und Risiken für die Einrichtungen der EU unerlässlich ist. Daher baut der vorgeschlagene Rahmen auf den Erfahrungen mit dem CSA1 auf und mobilisiert die Koordinierung der Informationsflüsse, um ein ganzheitliches Lagebild zu erstellen.

Die Bewertung des ECCF hat mehrere strategische Empfehlungen ergeben. Trotz der zentralen Rolle der ENISA bei der Förderung der Zusammenarbeit und des operativen Zusammenhalts zwischen den Mitgliedstaaten und anderen Interessenträgern ist die vor allem aufgrund der Komplexität der Verfahren zur Annahme der Systeme eingeschränkte Effizienz und Wirksamkeit des ECCF offensichtlich. Diese Probleme haben deutlich gemacht, dass die Governance-Strukturen grundlegend überarbeitet werden müssen, um die operative Klarheit und Rechenschaftspflicht auf allen Ebenen zu verbessern, was mit dem Vorschlag zur Überarbeitung des CSA angegangen wird. Die Erfahrungen mit der Funktionsweise des derzeitigen ECCF haben gezeigt, dass der Zertifizierungsrahmen modernisiert und präzisiert und ein Systempflegeverfahren für Zertifizierungssysteme eingeführt werden muss, damit diese dem Marktbedarf und der Bedrohungslandschaft entsprechen können. Schließlich wurden im ursprünglichen Rahmen nicht technische Risiken nicht vorhergesehen, die als Ursache für eine verzögerte Umsetzung des ECCF bei 5G- und Cloud-Systemen bestimmt werden können.

Die Komplexität des Cyber-Ökosystems der EU nimmt entsprechend den sich wandelnden Cyberbedrohungen zu. In den schriftlichen Beiträgen der Interessenträger bestand ein starker Konsens darüber, dass der Verwaltungsaufwand, insbesondere für KMU, verringert werden muss, und es wurden vereinfachte Befolgungsverfahren gefordert. Während die größten Vereinfachungsbemühungen über die Initiative für den Digital-Omnibus erfolgen werden, trägt der Vorschlag den Bedürfnissen der Interessenträger Rechnung, indem Änderungen an der NIS-2-Richtlinie eingeführt werden, sodass der Durchführungsprozess erleichtert wird.

1.5.4. Vereinbarkeit mit dem Mehrjährigen Finanzrahmen sowie mögliche Synergieeffekte mit anderen geeigneten Instrumenten

Mit der CSA2 werden die erforderlichen Überarbeitungen eingeführt, um die EU mit Instrumenten und Mechanismen auszustatten, mit denen auf die Cybersicherheitslandschaft und die politischen Ziele reagiert werden kann. Die vorgeschlagene Verordnung wird die ENISA mit den erforderlichen Fähigkeiten zur Unterstützung der Mitgliedstaaten bei der Umsetzung des EU-Rechts und bei der Abwehr von Cyberrisiken weiter stärken. Unter Berücksichtigung der bereits genannten Draghi- und Letta-Berichte stellt der Vorschlag für den mehrjährigen Finanzrahmen (MFR) 2028-2034 Wettbewerbsfähigkeit, Sicherheit und strategische Autonomie in den Mittelpunkt.

Infolgedessen werden mit den Vorschlägen im Rahmen des horizontalen Pakets zum MFR 2028-2034, insbesondere dem Europäischen Fonds für Wettbewerbsfähigkeit und den Vorschlägen zu Horizont Europa, neue Förderfähigkeitskriterien eingeführt, die auf dem Grundsatz des Ausschlusses von „Hochrisikoanbietern“ vom Erhalt von EU-Mitteln beruhen. Die CSA2 steht voll und ganz im Einklang mit diesem Grundsatz und stellt darüber hinaus ein Instrument dar, das die Umsetzung der neuen Anforderungen an „Hochrisikoanbieter“ ermöglicht, da es einen Verfahrensrahmen für die Benennung von Ländern bietet, für die auf EU-Ebene Cybersicherheitsbedenken bestehen. In dieser Hinsicht ist die CSA2 ein strategischer Vorschlag, der mit den Prioritäten der Kommission für die Verwirklichung der technologischen Souveränität und der Steigerung der Wettbewerbsfähigkeit in Europa im Einklang steht.

Die Überwindung der bestehenden Fragmentierung wird durch eine weitere Harmonisierung des EU-Zertifizierungsmarkts angegangen, wodurch das europäische Zertifizierungsverfahren effizienter und nachhaltiger gemacht wird.

In den MFR-Vorschlägen für 2028-2034 wird den Vereinfachungsbemühungen im gesamten Rahmen Priorität eingeräumt. Die Haushaltslinien werden von sieben auf vier komprimiert, während die Zahl der horizontalen Finanzierungsprogramme erheblich von 52 auf 16 verringert wurde, was für Flexibilität und die Fähigkeit zur Anpassung an den aktuellen Bedarf sorgt. In der Folgenabschätzung für die Überarbeitung des Rechtsakts zur Cybersicherheit wurden genau diese Ziele hervorgehoben: die Notwendigkeit, die Cybersicherheitsanforderungen über mehrere Rechtsrahmen hinweg zu vereinfachen sowie die Aufgaben der ENISA zu kodifizieren und auf die Bereiche zu konzentrieren, die die Resilienz des Cyberökosystems der EU am stärksten verbessern. Auf der Grundlage dieser Feststellungen fördern die vorgeschlagenen Bestimmungen die Wettbewerbsfähigkeit durch Vereinfachung, gewährleisten ein hohes Sicherheitsniveau durch verstärkte Koordinierung und Analyse von Risiken und Schwachstellen und unterstützen ein höheres Maß an Harmonisierung durch

Überwindung der Fragmentierung, die sich aus der Anzahl der nationalen Systeme ergibt. Darüber hinaus ist die ENISA als wichtigstes Instrument konzipiert, das die Bemühungen um eine digitale Vereinfachung vorantreiben wird, da sie die zentrale Anlaufstelle für Meldungen aufnehmen wird, wie in der Digital-Omnibus-Initiative[90] dargelegt.

Ein wesentlicher Bestandteil des MFR-Pakets 2028-2034 ist der Vorschlag für einen neuen Fonds für Wettbewerbsfähigkeit (ECF), der mehr als 16 Finanzierungsprogramme wie das Programm Digitales Europa (DEP), EU4Health, den Europäischen Verteidigungsfonds usw. unter einem Dach vereint. Das Programm Horizont Europa (HEP) wird weiterhin ein eigenständiges Programm sein, das eng mit dem ECF verknüpft ist. Dieser neue Programmplanungsrahmen erfordert eine starke Koordinierung und Finanzierung, die den aktuellen Prioritäten entspricht. In diesem Sinne bilden die vorgeschlagenen Bestimmungen der CSA2 die Grundlage für die Vertiefung der Koordinierung zwischen der ENISA und dem ECCC, die für die Programmumsetzung der cybersicherheitsbezogenen Teile des DEP und des HEP zuständig sind. Die vorgeschlagenen Bestimmungen sorgen für Kohärenz und heben die Synergien zwischen der ENISA und dem ECCC hervor. Dasselbe Konzept wurde auch bei der Zusammenarbeit mit anderen Agenturen und Stellen wie Europol verfolgt.

Ein weiterer Aspekt der Angleichung des CSA2-Vorschlags und des MFR 2028-2034 ist der Grundsatz der Flexibilität. Mit der Überarbeitung schlägt die Kommission einen „Gebührenmechanismus“ vor, der der ENISA eine flexible Möglichkeit bietet, einen Teil ihrer Tätigkeiten zu finanzieren, insbesondere im Zusammenhang mit der Entwicklung und Pflege von Systemen zur Bescheinigung von Cybersicherheitskompetenzen, der Bearbeitung und Erteilung von Befugnissen für Anbieter und der Pflege europäischer Systeme für die Cybersicherheitszertifizierung. Mit dieser Änderung wird die Agentur über die Flexibilität und Skalierbarkeit verfügen, um den Bedürfnissen der Interessenträger gerecht zu werden und durch die Refinanzierung ihrer Dienste nachhaltige Ausgaben zu tätigen.

1.5.5. Bewertung der verschiedenen verfügbaren Finanzierungsoptionen, einschließlich der Möglichkeiten für eine Umschichtung

Seit der letzten Überarbeitung des Mandats der ENISA im Jahr 2019 ist ein Trend hin zu einem exponentiellen Wachstum der erwarteten Beiträge der Agentur zur Unterstützung der Umsetzung des EU-Rechts zu verzeichnen. Dies führte zu Anträgen auf jährliche Mittel- und Personalaufstockungen über das ursprünglich geplante Niveau hinaus. Mit der vorgeschlagenen Überarbeitung werden wichtige neue Aufgaben eingeführt und Aufgaben in das Mandat der ENISA aufgenommen, die durch andere Rechtsakte nach der Annahme des CSA1 übertragen wurden, wodurch die Kapazitäten der ENISA erweitert werden, was zusätzliche finanzielle und personelle Aufstockungen erfordert. Ausgehend von dem Ziel, die digitale Sicherheit zum Wettbewerbsvorteil Europas zu machen, wird in dem Vorschlag eine echte Wirkung innerhalb des Cyber-Ökosystems gefordert. Dies wäre nur mit erheblichen Investitionen möglich, die den gewünschten Effekt erzielen und vor allem dem Bedarf der Mitgliedstaaten und anderer Interessenträger entsprechen. Im Rahmen der neuen Aufgaben werden technisches und spezialisiertes Personal sowie

[90] Bei Veröffentlichung einfügen.

finanzielle Investitionen (z. B. für Instrumente und Plattformen) benötigt, die nur durch zusätzliche Mittelzuweisungen aus dem EU-Haushalt sichergestellt werden könnten.

Mit dem Ziel einer größeren Flexibilität und gleichzeitig eines langfristig tragfähigen Haushalts der Agentur wird in der Überarbeitung ein Gebührenmechanismus vorgeschlagen, mit dem die Dienste, die für die Pflege des Rahmens für die Cybersicherheitszertifizierung und in Bezug auf die Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen sowie die Bearbeitung und Erteilung von Befugnissen für Anbieter erbracht werden, teilweise finanziert werden.

Alle Schätzungen für zusätzliche Ressourcen bei der Überarbeitung des CSA werden aus der Perspektive des Ausgangsbudgets der ENISA im Jahr 2025 (operative Kosten und VZÄ) vorgenommen. Die Kommission hat eine umfassende Analyse der Umschichtungsmöglichkeiten innerhalb der Agentur vorgenommen, um den im überarbeiteten Mandat vorgesehenen neuen Aufgaben gerecht zu werden. Die Tatsache, dass die Agentur an den Grenzen ihrer Kapazitäten arbeitet, ohne dass es Möglichkeiten zur Reduzierung von Aufgaben gibt, und dass der Verwaltungsrat bereits 2023 eine Maßnahme zur Aufhebung der Prioritäten ergriffen hat, führt eindeutig zu dem Schluss, dass im Rahmen der derzeitigen Struktur keine neuen Aufgaben bewältigt werden können, ohne dass sowohl die Haushaltsmittel als auch die Personalressourcen aufgestockt werden. Darüber hinaus werden viele der derzeitigen Aufgaben durch Beitragsvereinbarungen zwischen der ENISA und der Kommission abgedeckt. Daher zielt der Vorschlag darauf ab, diese Aufgaben in das Mandat der ENISA aufzunehmen und für die kommenden Jahre ein stabiles Budget zu erhalten.

Unbeschadet der Verhandlungen über den nächsten MFR werden die der Agentur ab 2028 zugewiesenen Mittel durch Umschichtungen aus Programmen im Rahmen des MFR 2028-2034 ausgeglichen. Wird eine Ausgleichskürzung erforderlich, müssen die der Agentur zugewiesenen Mittel und ihre Finanzierungsströme und -quellen möglicherweise überprüft werden. Die im vorgeschlagenen CSA2-Rahmen eingeführten Maßnahmen umfassen auch die Übernahme zusätzlicher Aufgaben für die Partner-GD der ENISA (Generaldirektion Kommunikationsnetze, Inhalte und Technologien, GD CNECT). Es sei insbesondere darauf hingewiesen, dass der Rahmen für die IKT-Lieferketten vollständig auf Kommissionsebene umgesetzt wird, einschließlich der Marktanalyse, die den Risikobewertungen beigefügt wird, und der Ausarbeitung von Durchführungsrechtsakten. Darüber hinaus werden zusätzliche Durchführungsrechtsakte in Bezug auf die Modalitäten der Gebührenmechanismen erforderlich sein, die die Kommission ausarbeitet und erlässt. Für die Durchsetzung des europäischen Rahmens für die Cybersicherheitszertifizierung, die Entwicklung von Musterbestimmungen, die Pflege von Cybersicherheitssystemen, Abkommen über die gegenseitige Anerkennung mit Drittländern und die Beaufsichtigung durch die ENISA wird eine zusätzliche Aufsicht und Unterstützung auf Kommissionsebene erforderlich sein.

1.6. Laufzeit der vorgeschlagenen Maßnahme/der Initiative und Dauer der finanziellen Auswirkungen

☐ **Befristete Laufzeit**

– ☐ Laufzeit: [TT.MM.]JJJJ bis [TT.MM.]JJJJ

– ☐ Finanzielle Auswirkungen auf die Mittel für Verpflichtungen von JJJJ bis JJJJ und auf die Mittel für Zahlungen von JJJJ bis JJJJ

☒ **Unbefristete Laufzeit**

– Anlaufphase von JJJJ bis JJJJ

– Anschließend reguläre Umsetzung

1.7. Vorgeschlagene Haushaltsvollzugsart(en)

☐ **Direkte Mittelverwaltung** durch die Kommission

– ☐ über ihre Dienststellen, einschließlich ihres Personals in den EU-Delegationen

– ☐ über Exekutivagenturen

☐ **Geteilte Mittelverwaltung** mit Mitgliedstaaten

☒ **Indirekte Mittelverwaltung** durch Übertragung von Haushaltsvollzugsaufgaben an:

– ☐ Drittländer oder die von ihnen benannten Einrichtungen

– ☐ internationale Einrichtungen und deren Agenturen (bitte angeben)

– ☐ die Europäische Investitionsbank und den Europäischen Investitionsfonds

– ☒ Einrichtungen im Sinne der Artikel 70 und 71 der Haushaltsordnung

– ☐ öffentlich-rechtliche Körperschaften

– ☐ privatrechtliche Einrichtungen, die im öffentlichen Auftrag tätig werden, sofern ihnen ausreichende finanzielle Garantien bereitgestellt werden

– ☐ privatrechtliche Einrichtungen eines Mitgliedstaats, die mit der Einrichtung einer öffentlich-privaten Partnerschaft betraut werden und denen ausreichende finanzielle Garantien bereitgestellt werden

– ☐ Einrichtungen oder Personen, die mit der Durchführung bestimmter Maßnahmen im Bereich der Gemeinsamen Außen- und Sicherheitspolitik im Rahmen des Titels V des Vertrags über die Europäische Union betraut und die in dem maßgeblichen Basisrechtsakt benannt sind

– ☐ in einem Mitgliedstaat ansässige Einrichtungen, die dem Privatrecht eines Mitgliedstaats oder dem Unionsrecht unterliegen und im Einklang mit sektorspezifischen Vorschriften für die Betrauung mit der Ausführung von Unionsmitteln oder mit der Erteilung von Haushaltsgarantien in Betracht kommen, insofern diese Einrichtungen von privatrechtlichen, im öffentlichen Auftrag tätig werdenden Einrichtungen kontrolliert und von den Kontrollstellen mit angemessenen finanziellen Garantien mit gesamtschuldnerischer Haftung oder gleichwertigen finanziellen Garantien ausgestattet werden, die bei jeder Maßnahme auf den Höchstbetrag der Unionsunterstützung begrenzt sein können.

Bemerkungen

2. VERWALTUNGSMAßNAHMEN

2.1. Überwachung und Berichterstattung

Die Überwachung und die Berichterstattung erfolgen nach den Grundsätzen des bestehenden CSA[91], der Haushaltsordnung[92] sowie im Einklang mit dem Gemeinsamen Konzept für die dezentralen Agenturen[93].

Gemäß Artikel 40 der Haushaltsordnung muss die ENISA der Kommission, dem Europäischen Parlament und dem Rat jedes Jahr ein einheitliches Programmplanungsdokument übermitteln, das die Mehrjahres- und Jahresprogramme und die Ressourcenplanung enthält. Darüber hinaus wird mit dem Vorschlag der Kommission zur Änderung des ENISA-Mandats die Anforderung eingeführt, dass die Kommission als Mitglied des Verwaltungsrats für die Annahme des einheitlichen Programmplanungsdokuments durch den Verwaltungsrat der ENISA in Personal- und Haushaltsfragen ein positives Votum abgibt. Die Kommission wird außerdem eine Stellungnahme zum Entwurf des einheitlichen Programmplanungsdokuments abgeben, bevor das Abstimmungsverfahren im Verwaltungsrat stattfindet, der vor der Annahme des einheitlichen Programmplanungsdokuments nachgekommen werden sollte[94].

Die ENISA muss dem Verwaltungsrat einen konsolidierten jährlichen Tätigkeitsbericht vorlegen. Dieser Bericht enthält insbesondere Informationen über die Verwirklichung der im einheitlichen Programmplanungsdokument festgelegten Ziele und Ergebnisse. Der Bericht ist auch der Kommission, dem Europäischen Parlament und dem Rat zu übermitteln. Der Exekutivdirektor der ENISA sollte dem Verwaltungsrat alle zwei Jahre eine Ex-post-Bewertung der Tätigkeiten der ENISA vorlegen. Außerdem sollte die Agentur einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen nachträglicher Bewertungen erstellen und der Kommission alle zwei Jahre über die Fortschritte berichten. Der Verwaltungsrat sollte dafür zuständig sein, die angemessene Weiterbehandlung der Schlussfolgerungen zu überwachen.

Behauptete Missstände bei der Tätigkeit der Agentur können vom Europäischen Bürgerbeauftragten nach Artikel 228 des Vertrags über die Arbeitsweise der Europäischen Union untersucht werden.

Die Daten für die geplante Überwachung würden überwiegend von der ENISA, der Europäischen Gruppe für die Cybersicherheitszertifizierung, der NIS-Kooperationsgruppe, dem CSIRTs-Netzwerk und den Behörden der Mitgliedstaaten stammen. Neben den Daten aus den Berichten (einschließlich der jährlichen Tätigkeitsberichte) der ENISA, der Europäischen Gruppe für die Cybersicherheitszertifizierung, der NIS-Kooperationsgruppe, des CSIRTs-Netzwerks und der Kommission werden im Bedarfsfall spezielle Datenerfassungsinstrumente verwendet werden (z. B. Umfragen bei nationalen Behörden, Eurobarometer, spezielle Studien und Berichte über europaweite Übungen).

91 Der EU-Rechtsakt zur Cybersicherheit |EUR-Lex.

92 Haushaltsordnung für den Gesamthaushaltsplan der Union (Neufassung), Amt für Veröffentlichungen der Europäischen Union.

93 https://europa.eu/european-union/sites/europaeu/files/docs/body/joint_statement_and_common_approach_2012_en.pdf.

94 Delegierte Verordnung (EU) 2019/715 – DE – EUR-Lex.

Mit dem Vorschlag der Kommission für die CSA2 wird die etablierte Überprüfungspraxis und Bewertung der Agentur fortgesetzt. Wie in Artikel 119 des CSA2-Vorschlags dargelegt, muss die Kommission bis zum [TT.MM.JJJJ] und danach alle fünf Jahre eine Bewertung der ENISA veranlassen. Gegenstand dieser Bewertung sind insbesondere das etwaige Erfordernis, das Mandat der ENISA zu ändern, sowie die finanziellen Auswirkungen einer solchen Änderung. Bei jeder zweiten Bewertung werden die von der ENISA erzielten Ergebnisse im Hinblick auf ihre Ziele, ihr Mandat, ihren Auftrag, ihre Leitung und ihre Aufgaben betrachtet, einschließlich einer Bewertung der Frage, ob die Weiterführung der ENISA im Hinblick auf diese Ziele, dieses Mandat, diesen Auftrag, diese Leitung und diese Aufgaben noch gerechtfertigt ist.

Die Bewertung erstreckt sich auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III der Verordnung im Hinblick auf die Ziele des europäischen Rahmens für die Cybersicherheitszertifizierung, für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und Einrichtungen in der Union ein angemessenes Maß an Cybersicherheit und einen besser funktionierenden Binnenmarkt zu gewährleisten.

Gegenstand der Bewertung sin ferner die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels IV der Verordnung im Hinblick auf die Ziele des Rahmens für die Sicherheit der IKT-Lieferketten.

Die Kommission erstattet dem Europäischen Parlament und dem Rat über alle Feststellungen und dem Verwaltungsrat über die Ergebnisse der Bewertung in Bezug auf Titel II der Verordnung Bericht. Die Ergebnisse der Bewertung werden veröffentlicht.

2.2. Verwaltungs- und Kontrollsystem(e)

2.2.1. Begründung der Haushaltsvollzugsart(en), des Durchführungsmechanismus/der Durchführungsmechanismen für die Finanzierung, der Zahlungsmodalitäten und der Kontrollstrategie, wie vorgeschlagen

In Anbetracht der Tatsache, dass der Vorschlag Auswirkungen auf den jährlichen Beitrag der EU an die ENISA hat, wird der EU-Haushalt über eine indirekte Verwaltung ausgeführt werden.

Gemäß dem Grundsatz der Wirtschaftlichkeit der Haushaltsführung wird der Haushalt der ENISA unter Gewährleistung einer effizienten und wirksamen internen Kontrolle ausgeführt. Daher ist die ENISA an die Umsetzung einer angemessenen Kontrollstrategie gebunden, die mit allen maßgeblichen Akteuren der Kontrollkette abgestimmt wird.

Hinsichtlich der Ex-post-Kontrollen ist die ENISA als dezentrale Agentur insbesondere Gegenstand

– einer internen Prüfung durch den Internen Auditdienst der Kommission,

– von Jahresberichten des Europäischen Rechnungshofs, die eine Erklärung über die Zuverlässigkeit der Rechnungsführung sowie die Rechtmäßigkeit und Ordnungsmäßigkeit der zugrunde liegenden Vorgänge enthalten,

– einer jährlichen Entlastung durch das Europäische Parlament,

– von möglichen Untersuchungen durch das OLAF, um insbesondere sicherzustellen, dass die den Agenturen zugewiesenen Mittel ordnungsgemäß eingesetzt werden.

– Als Partner-GD der ENISA wird die GD CNECT ihre Kontrollstrategie auf die dezentralen Agenturen anwenden, um für eine verlässliche Berichterstattung im Rahmen ihres jährlichen Tätigkeitsberichts Sorge zu tragen. Während die dezentralen Agenturen die volle Verantwortung für die Ausführung ihres Haushaltsplans tragen, ist die GD CNECT für die regelmäßige Zahlung der von der Haushaltsbehörde festgelegten jährlichen Beiträge zuständig.

– Schließlich sorgt der Europäische Bürgerbeauftragte für eine weitere Ebene der Kontrolle und Rechenschaftspflicht in Bezug auf die ENISA.

Auf der Grundlage der Bewertung der Agentur und der Folgenabschätzung, die zur Vorlage des CSA2-Vorschlags durchgeführt wurde, wurde festgestellt, dass es von größter Bedeutung ist, angemessene Finanzmittel sicherzustellen, damit die ENISA die ihr durch das neue Mandat übertragenen Aufgaben erfüllen kann. Eine wichtige Neuerung im Zuge des überarbeiteten Mandats der Agentur wird die Einführung eines Gebührenmechanismus sein, mit dem die Kosten für die Pflege der im Rahmen des ECCF angenommenen europäischen Systeme für die Cybersicherheitszertifizierung finanziert werden sollen. Mit dem überarbeiteten ECCF wird das Systempflegeverfahren formalisiert. Die Systempflegetätigkeit wird von der ENISA geleitet und teilweise durch Gebühren finanziert, um ihrem skalierbaren Charakter Rechnung zu tragen (mehr Systeme benötigen mehr Personal für die Systempflege). Die Agentur wird auch in der Lage sein, Testinstrumente bereitzustellen, um die Durchführung von Konformitätsbewertungsverfahren sowohl im Rahmen des ECCF als auch anderer einschlägiger EU-Rechtsvorschriften im Cyberbereich zu unterstützen. Die Modalitäten der Gebühren werden in einem Durchführungsrechtsakt festgelegt, der von der Kommission erlassen wird. Darüber hinaus sieht die Überarbeitung die Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen und das Treffen von Entscheidungen zur Erteilung der Befugnis an Anbieter zur Ausstellung europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen vor.

2.2.2. Angaben zu den ermittelten Risiken und dem/den zu deren Eindämmung eingerichteten System(en) der internen Kontrolle

Der CSA2-Vorschlag als solcher zielt darauf ab, die im Rahmen des Mandats der ENISA und des ECCF ermittelten Risiken, einschließlich des Rahmens für die Sicherheit der IKT-Lieferketten und der Vereinfachungsbestimmungen, zu mindern. Konkret handelt es sich bei der ENISA um eine bereits bestehende Agentur der Europäischen Union, und im Zuge der Überarbeitung wird das Mandat weiter präzisiert, indem die Bereiche gestärkt werden, in denen die Agentur einen klaren Mehrwert gezeigt hat, und indem neue Bereiche hinzugefügt werden, in denen angesichts der neuen politischen Prioritäten und Instrumente Unterstützung benötigt wird, wie z. B. Vereinfachung durch die Aufnahme einer zentralen Anlaufstelle für die Meldung, Unterstützung eines gemeinsamen europäischen Lagebilds und der operativen Zusammenarbeit sowie Stärkung und Straffung des europäischen Rahmens für die Cybersicherheitszertifizierung.

Ein weiteres ermitteltes Risiko, auf das in dem Vorschlag eingegangen wird, ist die Zahl der Beitragsvereinbarungen, die die Kommission und die Agentur in den letzten Jahren geschlossen haben. Aufgrund der derzeitigen geopolitischen Lage und der

sich rasch wandelnden Bedrohungslage im Bereich der Cybersicherheit hat die Kommission seit 2019 Beitragsvereinbarungen mit der Agentur im Wert von insgesamt mehr als 75 Mio. EUR geschlossen. Da die der ENISA in diesen Vereinbarungen übertragenen Aufgaben inzwischen dauerhafter Natur sind, stellt der instabile Mittelfluss durch Beitragsvereinbarungen ein Risiko für die langfristige Erbringung der Ergebnisse der Tätigkeiten der ENISA dar.

Daher zielt der vorliegende Vorschlag unter anderem darauf ab, die Ressourcenkapazitäten der Agentur zu stärken, ihre Aufgaben neu zu definieren und Effizienzgewinne zu erzielen. Insbesondere wird die Möglichkeit, Gebühren zu erheben, langfristig einen tragfähigen Finanzkreislauf der Agentur unterstützen, indem die Kosten im Zusammenhang mit der Pflege der im Rahmen des ECCF angenommenen europäischen Zertifizierungssysteme, der Erprobung von Instrumenten und der Entwicklung, Pflege und Umsetzung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen refinanziert werden. Langfristig dürften Einsparungen für den EU-Haushalt in Höhe von 18,5 Mio. EUR pro Jahr erzielt werden. Die Kommission wird bei den Modalitäten der Gebühren und deren Zusammensetzung durch den Erlass von Durchführungsrechtsakten federführend sein.

Die Zunahme der operativen Aufgaben der Agentur stellt kein wirkliches Risiko dar. Durch diese Aufgaben würden die Maßnahmen der Mitgliedstaaten ergänzt und auf Anfrage unterstützt. Analog zum Rechtsakt zur Cybersicherheit (EU) 2019/881[95] werden sie ebenfalls auf vordefinierte Dienste beschränkt sein. Die neuen Elemente/Aufgaben des Vorschlags werden einen Mehrwert für die europäischen Interessenträger mit sich bringen, die davon profitieren würden, wenn die ENISA als Informationsdrehscheibe fungieren, zur Informationsweitergabe beitragen und ihnen Warnmeldungen zukommen lassen würde.

Darüber hinaus steht das vorgeschlagene Modell der Agentur im Einklang mit dem Gemeinsamen Konzept der Kommission für dezentrale Agenturen, wodurch sichergestellt wird, dass es eine ausreichende Kontrolle gibt, um abzusehen, dass die ENISA auf ihre Ziele hinarbeitet. Die operativen und finanziellen Risiken der vorgeschlagenen Änderungen scheinen begrenzt zu sein, da die Bestimmungen dazu dienen, die derzeitigen Risiken zu mindern. Dennoch könnten langfristig gewisse negative Aspekte eintreten, und zwar in Bezug auf Folgendes:

– angespannte Lage in Bezug auf operative Mittel aufgrund des steigenden operativen Bedarfs der Mitgliedstaaten und sich ständig weiterentwickelnder Cyberrisiken und Bedrohungen im Bereich der Cybersicherheit;

– rasche Aufstockung der Mittel und Erwartung einer ebenso raschen Ausführung;

– Mangel an angemessenen finanziellen und personellen Ressourcen, um dem operativen Bedarf gerecht zu werden.

[95] https://eur-lex.europa.eu/eli/reg/2019/881/oj/deu.

2.2.3. Schätzung und Begründung der Kosteneffizienz der Kontrollen (Verhältnis zwischen den Kontrollkosten und dem Wert der betreffenden verwalteten Mittel) sowie Bewertung des erwarteten Ausmaßes des Fehlerrisikos (bei Zahlung und beim Abschluss)

Die Kosten, die der GD CNECT für die Überwachung und Beaufsichtigung der betrauten Einrichtungen, einschließlich der ENISA, entstehen, belaufen sich laut dem jährlichen Tätigkeitsbericht für 2024[96] auf rund 5,25 Mio. EUR. Dieser Betrag umfasst in erster Linie Personalkosten und macht 0,50 % der im Jahr 2024 an diese Einrichtungen geleisteten operativen Zahlungen aus. Die Gesamtquote der Kontrollkosten stieg leicht von 0,46 % im Jahr 2023 auf 0,50 % im Jahr 2024, bleibt aber im Vergleich zu den Vorjahren relativ stabil.

Genauer gesagt, belaufen sich die Kontrollkosten, was die ENISA betrifft, im Jahr 2024 auf 0,32 Mio. EUR bzw. 0,70 % Kontrollkosten im Vergleich zu 0,69 % im Jahr 2023 und 1,22 % im Jahr 2022. Die Analyse zeigt, dass höhere Kontrollkosten in erster Linie mit der Vorbereitung und Überwachung von Beitragsvereinbarungen zwischen der Kommission und der Agentur verbunden sind (hauptsächlich Personalkosten), die mit dem neuen Mandat erheblich gesenkt werden dürften, was somit ein höheres Maß an Effizienz erwarten lässt. Was die Gesamtkosten für die GD CNECT im Vergleich zu den anderen betrauten Einrichtungen betrifft, so befindet sich die ENISA im Vergleich zu elf anderen Einrichtungen im Mittelfeld.

Der CSA2-Vorschlag sieht eine Aufstockung des Personals der GD CNECT um 50 VZÄ vor, von denen ein zusätzliches VZÄ speziell für die Aufgaben im Zusammenhang mit der GD CNECT als Partner-GD der Agentur zugewiesen wird. Diese Person wird die Ausarbeitung einer Stellungnahme der Kommission zum einheitlichen Programmplanungsdokument der ENISA und die Überwachung von dessen Umsetzung sowie die Beaufsichtigung der Erstellung des Haushaltsplans der Agentur und dessen Ausführung unterstützen. Unterstützung der Agentur bei der Entwicklung ihrer Tätigkeiten gemäß den Strategien der Union, u. a. durch Teilnahme an relevanten Sitzungen. Die Maßnahme ist durch die erweiterten Überwachungsaufgaben der GD CNECT gerechtfertigt, in deren Rahmen unter anderem vorgesehen ist, dass die Kommission in Haushalts- und Personalfragen ein positives Votum abgibt. Es sei darauf hingewiesen, dass die Umsetzung der Bestimmungen in Bezug auf die Benennung von Ländern, von denen strategische Cybersicherheitsrisiken für bestimmte wichtige Assets ausgehen, und Hochrisikoanbieter vollständig in Hand der Kommission liegt. Der geschätzte Personalbedarf für die Risikobewertungen im Zusammenhang mit den oben genannten Tätigkeiten beläuft sich auf 25 VZÄ. Die Maßnahme ist durch den Umfang der Arbeiten gerechtfertigt, die zur Umsetzung des politischen Rahmens erforderlich sind, insbesondere die Unterstützung koordinierter Risikobewertungen der EU, die wirtschaftliche Analyse für jedes IKT-Produkt/jede IKT-Dienstleistung, die Ausarbeitung der entsprechenden Durchführungsrechtsakte und die Verfolgung der Umsetzung des Rahmens, die Durchführung von Bewertungen der Eigentums- und Kontrollverhältnisse. Die Kosten der Kontrollen, die der Kommission durch die Umsetzung des Rahmens für die Lieferketten entstehen, dürften wohl insbesondere von der Zahl der von der Kommission durchgeführten Bewertungen der Eigentums- und Kontrollverhältnisse abhängen. Die hierbei erzielten Ergebnisse werden jedoch

96 CNECT_AAR_2024_final.

erheblich zu Einsparungen für die Mitgliedstaaten bei der Beaufsichtigung der Umsetzung von Abhilfemaßnahmen und Verpflichtungen beitragen, die den NIS-2-Einrichtungen durch den Rahmen auferlegt werden. Die Mitgliedstaaten werden die Ergebnisse der Bewertungen der Eigentums- und Kontrollverhältnisse direkt nutzen können, anstatt jeweils einzeln Ressourcen für denselben Bewertungsbedarf aufzuwenden. Die Stärkung des europäischen Rahmens für die Cybersicherheitszertifizierung, die Normung und Durchführung damit verbundener Tätigkeiten sowie die Umsetzung der NIS-2-Richtlinie (einschließlich des jeweiligen Umsetzungsbedarfs, der Durchführungsrechtsakte zu Gebühren und der Unterstützung der Pflege der Zertifizierungssysteme und Kompetenzbescheinigungssysteme) erfordert Schätzungen zufolge 19 VZÄ, während für die operative Zusammenarbeit und die Maßnahmen zur Lageerfassung zusätzliche 5 VZÄ erforderlich sind. Vollständige Beschreibung der Aufgaben in Abschnitt 3.2.4.

Die ENISA gelangte in ihrem konsolidierten jährlichen Tätigkeitsbericht 2023[97] zu einer positiven Bewertung ihrer internen Kontrollsysteme und legte eine einwandfreie Zuverlässigkeitserklärung vor. In seinem Jahresbericht über die Agenturen der EU für das Haushaltsjahr 2023 gab der Europäische Rechnungshof ein einwandfreies Prüfungsurteil uneingeschränktes Prüfungsurteil zur Jahresrechnung und ein eingeschränktes Prüfungsurteil zur Rechtmäßigkeit und Ordnungsmäßigkeit der der Jahresrechnung zugrunde liegenden Zahlungen ab (siehe auch Abschnitt 2.2.2). Die GD CNECT hat den Bericht zur Kenntnis genommen, kam jedoch zu dem Schluss, dass er keine Auswirkungen auf die Wirksamkeit der Aufsicht durch CNECT hat. Die ENISA berichtet ferner regelmäßig über die Maßnahmen, die ergriffen wurden, um ein erneutes Auftreten der Feststellungen zu verhindern, und bisher gibt es keine Anzeichen dafür, dass sich die Fehlerquote in den kommenden Jahren verschlechtern/über 2 % liegen wird.

Darüber hinaus sieht Artikel 80 Absatz 2 der Finanzregelung für die ENISA[98] die Möglichkeit vor, dass die Agentur eine interne Rechnungsprüfung mit anderen, in demselben Politikbereich tätigen Unionseinrichtungen teilen kann, wenn die interne Rechnungsprüfung einer einzigen Unionseinrichtung nicht kosteneffizient ist.

Zusammenfassend lässt sich sagen, dass sich aus der Analyse angesichts der vorgeschlagenen Vergrößerung der Agentur um mehr als 100 % im Vergleich zur relativ geringen Erhöhung der Kontrollkosten ein zufriedenstellendes Kosten-Nutzen-Verhältnis ergibt. Unter Berücksichtigung aller verfügbaren Daten gibt es keinen Hinweis darauf, dass der erwartete Fehler über 2 % liegen könnte.

2.3. Prävention von Betrug und Unregelmäßigkeiten

Die Agentur der Europäischen Union für Cybersicherheit wird die höchsten Standards zur Verhinderung von Betrug und Unregelmäßigkeiten anwenden.

Zahlungen für die angeforderten Dienstleistungen oder Studien werden von den Bediensteten der Agentur vor der Zahlung unter Berücksichtigung etwaiger vertraglicher Verpflichtungen, wirtschaftlicher Grundsätze und einer guten Finanz- oder Verwaltungspraxis überprüft. In alle Vereinbarungen und Verträge zwischen der Agentur und den Zahlungsempfängern werden Bestimmungen zur ein

97 enisa.europa.eu/sites/default/files/2024-11/2023 Consolidated Annual Activity Report_1.pdf.

98 MB Decision 2019_8 Financial rules_adopted.pdf.

Betrugsbekämpfung (Beaufsichtigung, Verpflichtung zur Berichterstattung usw.) aufgenommen.

Für die Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gelten uneingeschränkt die Bestimmungen der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates.

3. GESCHÄTZTE FINANZIELLE AUSWIRKUNGEN DES VORSCHLAGS/DER INITIATIVE

3.1. Betroffene Rubrik(en) des Mehrjährigen Finanzrahmens und Ausgabenlinie(n) im Haushaltsplan

- Bestehende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beiträge			
	Nummer	GM/NGM [99]	von EFTA-Ländern [100]	von Kandidatenländern und potenziellen Kandidaten [101]	von anderen Drittländern	andere zweckgebundene Einnahmen
	[XX.YY.YY.YY]	NGM	JA	NEIN	NEIN	JA/NEIN
	[XX.YY.YY.YY]	GM/NGM	JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN
	[XX.YY.YY.YY]	GM/NGM	JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

- Neu zu schaffende Haushaltslinien

In der Reihenfolge der Rubriken des Mehrjährigen Finanzrahmens und der Haushaltslinien.

Rubrik des Mehrjährigen Finanzrahmens	Haushaltslinie	Art der Ausgaben	Beiträge			
	Nummer	GM/NGM	von EFTA-Ländern	von Kandidatenländern und potenziellen Kandidaten	von anderen Drittländern	andere zweckgebundene Einnahmen

[99] GM = Getrennte Mittel/NGM = Nichtgetrennte Mittel.
[100] EFTA: Europäische Freihandelsassoziation.
[101] Kandidatenländer und gegebenenfalls potenzielle Kandidaten des Westbalkans.

	[XX.YY.YY.YY]	GM/NGM	JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN
	[XX.YY.YY.YY]	GM/NGM	JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN
	[XX.YY.YY.YY]	GM/NGM	JA/NEIN	JA/NEIN	JA/NEIN	JA/NEIN

3.2. Geschätzte finanzielle Auswirkungen des Vorschlags auf die Mittel

3.2.1 Übersicht über die geschätzten Auswirkungen auf die operativen Mittel

– ☐ Für den Vorschlag/die Initiative werden keine operativen Mittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden operativen Mittel benötigt:

3.2.1.1. Mittel aus dem verabschiedeten Haushaltsplan

in Mio. EUR (3 Dezimalstellen)

Agentur: ENISA	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**MFR 2028-2034 INSGESAMT**
Haushaltslinie: <…….> / zusätzlicher Beitrag aus dem EU-Haushalt, der der Agentur zugutekommt	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006

Die Mittel/der Beitrag aus dem EU-Haushalt, die/der der Agentur zugutekommen/zugutekommt, wird durch eine entsprechende Kürzung der Mittelausstattung für das Programm <….>/die Haushaltslinie ausgeglichen: <….>/im Jahr/in den Jahren: <…….> .

			Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**MFR 2028-2034 INSGESAMT**
Operative Mittel INSGESAMT	Verpflichtungen	(4)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006
	Zahlungen	(5)	20,900	20,594	25,338	26,801	26,801	26,301	26,301	173,006
Aus der Dotation bestimmter spezifischer Programme finanzierte Verwaltungsmittel INSGESAMT		(6)	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**

Mittel INSGESAMT unter der RUBRIK 2 des Mehrjährigen Finanzrahmens	Verpflichtungen	= 4+6	22,265	21,959	26,808	28,586	28,901	28,716	28,926	186,161
	Zahlungen	= 5+6	22,265	20,890	24,851	26,254	26,254	25,754	25,754	186,161

GD CNECT	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**MFR 2028-2034 INSGESAMT**
• Personalausgaben	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**
• Sonstige Verwaltungsausgaben	0	0	0	0	0	0	0	**0**

GD CNECT **INSGESAMT**	Mittel	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

Mittel INSGESAMT unter der RUBRIK 4 des Mehrjährigen Finanzrahmens	(Verpflichtungen insges. = Zahlungen insges.)	**2,328**	**2,328**	**3,104**	**3,492**	**3,880**	**4,268**	**4,850**	**24,25**

in Mio. EUR (3 Dezimalstellen)

		Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**MFR 2028-2034 INSGESAMT**
Mittel INSGESAMT unter den RUBRIKEN 1	Verpflichtungen	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

bis 4										
des Mehrjährigen Finanzrahmens	Zahlungen	24,594	24,257	29,912	32,078	32,781	32,984	33,776	210,38

3.2.2. Geschätzter Output, der mit operativen Mitteln finanziert wird (nicht auszufüllen im Fall dezentraler Agenturen)

Mittel für Verpflichtungen, in Mio. EUR (3 Dezimalstellen)

Ziele und Outputs angeben ⇩			Jahr **2028**		Jahr **2029**		Jahr **2030**		Jahr **2031**		Bei länger andauernden Auswirkungen bitte weitere Spalten einfügen (siehe 1.6)						**INSGESAMT**	
	OUTPUTS																	
	Art[102]	Durchschnittskosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Anzahl	Kosten	Gesamtzahl	Gesamtkosten
EINZELZIEL Nr. 1[103]…																		
- Output																		
- Output																		
- Output																		
Zwischensumme für Einzelziel Nr. 1																		
EINZELZIEL Nr. 2...																		
- Output																		
Zwischensumme für Einzelziel Nr. 2																		

102 Outputs sind Produkte, die geliefert, und Dienstleistungen, die erbracht werden (z. B. Zahl der Austauschstudenten, gebaute Straßenkilometer usw.).

103 Wie in Abschnitt 1.3.2. beschrieben. „Einzelziel(e)“

INSGESAMT																

3.2.3. Übersicht über die geschätzten Auswirkungen auf die Verwaltungsmittel

– ☐ Für den Vorschlag/die Initiative werden keine Verwaltungsmittel benötigt.

– ☒ Für den Vorschlag/die Initiative werden die folgenden Verwaltungsmittel benötigt:

3.2.3.1. Mittel aus dem verabschiedeten Haushaltsplan

(zusätzlich)

BEWILLIGTE MITTEL	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**2028-2034 INSGESAMT**
RUBRIK 4								
Personalausgaben	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Sonstige Verwaltungsausgaben	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
Zwischensumme RUBRIK 4	2,328	2,328	3,104	3,492	3,880	4,268	4,840	24,25
Außerhalb der RUBRIK 4								
Personalausgaben	1,365	1,365	1,470	1,785	2,100	2,415	2,625	**13,125**
Sonstige Verwaltungsausgaben	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Zwischensumme außerhalb der RUBRIK 4	**1,365**	**1,365**	**1,470**	**1,785**	**2,100**	**2,415**	**2,625**	**13,125**
INSGESAMT	**3,693**	**3,693**	**4,574**	**5,277**	**5,980**	**6,683**	**7,475**	**37,375**

3.2.4. Geschätzter Personalbedarf (zusätzlich)

– ☐ Für den Vorschlag/die Initiative wird kein Personal benötigt.

– ☒ Für den Vorschlag/die Initiative wird das folgende Personal benötigt:

3.2.4.1. Finanziert aus dem verabschiedeten Haushalt

Schätzung in Vollzeitäquivalenten (VZÄ)[104]

BEWILLIGTE MITTEL	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**
• Planstellen (Beamte und Bedienstete auf Zeit)							
20 01 02 01 (Zentrale Dienststellen und Vertretungen der Kommission)	12	12	16	18	20	22	25
20 01 02 03 (EU-Delegationen)	0	0	0	0	0	0	0
(Indirekte Forschung)	0	0	0	0	0	0	0
(Direkte Forschung)	0	0	0	0	0	0	0
Sonstige Haushaltslinien (bitte angeben)	0	0	0	0	0	0	0
• Externes Personal (in VZÄ)							
20 02 01 (VB und ANS der Globaldotation)	0	0	0	0	0	0	0

104 Bitte unter der Tabelle angeben, wie viele der aufgeführten VZÄ bereits der Verwaltung der Maßnahme zugeordnet sind und/oder durch Personalumschichtung innerhalb der GD dieser Aufgabe zugeteilt werden können. Den Nettobedarf beziffern.

20 02 03 (VB, ÖB, ANS und JPD in den EU-Delegationen)		0	0	0	0	0	0	0
Haushaltslinie administr. Unterstützung	– in den zentralen Dienststellen	0	0	0	0	0	0	0
[XX.01.YY.YY]	– in den EU-Delegationen	0	0	0	0	0	0	0
(VB und ANS – indirekte Forschung)		0	0	0	0	0	0	0
(VB und ANS – direkte Forschung)		0	0	0	0	0	0	0
Sonstige Haushaltslinien (bitte angeben) – Rubrik 4		0	0	0	0	0	0	0
Sonstige Haushaltslinien (bitte angeben) – außerhalb der Rubrik 4		13	13	14	17	20	23	25
INSGESAMT		**25**	**25**	**30**	**35**	**40**	**45**	**50**

Für die Durchführung des Vorschlags benötigtes Personal (in VZÄ):

	Personal aus den Dienststellen der Kommission	**Zusatzpersonal (ausnahmsweise)**		
		Zu finanzieren aus Rubrik 7 oder Forschung	**Zu finanzieren aus einer Haushaltslinie für administrative Unterstützung**	**Zu finanzieren aus Gebühren**
Planstellen		25		
Externes Personal (VB, ANS, LAK)			25	

Die geschätzten Auswirkungen auf die Ausgaben und die Personalausstattung für 2028 und darüber hinaus sind vorläufig und greifen dem nächsten mehrjährigen Finanzrahmen nicht vor. Die Finanzierungsquelle und der Umfang der finanziellen Verpflichtung der Union in der Zeit nach 2027 hängen weiterhin vom Ergebnis der interinstitutionellen Verhandlungen über den MFR 2028-2034, dem jährlichen Haushaltsverfahren und dem Lenkungsmechanismus ab.

Beschreibung der von der GD innerhalb der Kommission auszuführenden Aufgaben

Beamte und Zeitbedienstete	**Koordinierung ENISA (1)**: Vertretung der Kommission im Verwaltungsrat der Agentur. Ausarbeitung einer Stellungnahme der Kommission zum einheitlichen Programmplanungsdokument der ENISA und Überwachung dessen Umsetzung. Beaufsichtigung der Erstellung des Haushaltsplans der Agentur und dessen Ausführung. Unterstützung der Agentur bei der Entwicklung ihrer Tätigkeiten gemäß den Strategien der Union, u. a. durch Teilnahme an relevanten Sitzungen. **Systeme zur Bescheinigung von Kompetenzen / Akademie für Kompetenzen (2)**: Bei CNECT wird zusätzliches Personal benötigt, um Durchführungsrechtsakte zur Festlegung der Gebühren auszuarbeiten, die die ENISA Antragstellern für die Zulassung als befugte Anbieter in Rechnung stellen wird. Dabei handelt es sich um mindestens 12 Durchführungsrechtsakte – einen pro ECSF-Profil.

	Lieferketten (25): Unterstützung bei der Vorbereitung der koordinierten Risikobewertungen der Union. Durchführung einer wirtschaftlichen Analyse für jede(s) betrachtete IKT-Produkt/-Dienstleistung. Ausarbeitung der jeweiligen Durchführungsrechtsakte zur Ermittlung der wichtigen Assets, zu vorgeschlagenen Risikominderungsmaßnahmen und zur Benennung von Ländern, von denen strategische Cybersicherheitsrisiken für bestimmte wichtige Assets ausgehen, Ermittlung von Hochrisikoanbietern, Überprüfung von Ausnahmeanträgen und Vorbereitung der Beschlüsse der Kommission. Unterstützung der Umsetzung und Beaufsichtigung der angenommenen Maßnahmen. **Europäischer Rahmen für die Cybersicherheitszertifizierung, Normung und Durchführung damit verbundener Tätigkeiten, Umsetzung der NIS-2-Richtlinie (17)**: Durchsetzung des CSA, insbesondere Governance der Konformitätsbewertungsstellen (Anfechtung der Zuständigkeit) Einbindung (und Versammlung) der Interessenträger Gegenseitige Anerkennung mit Drittländern Entwicklung eines standardisierten Durchführungsrechtsakts (detaillierte Anträge, die Gegenstand von Konsultationen sind, und Entwicklung von Musterbestimmungen) Systempflege, rechtliche Prüfung, Ausschussverfahren Koordinierung mit NIS-Kooperationsgruppe und Pflege des Systems von Einrichtungen Durchführungsrechtsakte im Rahmen der NIS-2-Richtlinie Angleichung der Konformitätsbewertungsstellen an die CSA, Konformitätsvermutung + Normung Koordinierung zwischen Marktüberwachungsbehörden und nationalen Behörden für die Cybersicherheitszertifizierung Technische Angleichung der Cyberresilienzverordnung und der Zertifizierungssysteme **Operative Koordinierung und Lageerfassung (5)**: Sektorspezifische Sachkenntnis und Sachkenntnis in Bezug auf Bedrohungsakteure als Beitrag zur Lageerfassung auf EU-Ebene im Hinblick auf Bedrohungen für kritische Infrastrukturen, auch durch neu aufkommende Technik Koordinierung mit der ENISA und anderen Einrichtungen und Netzwerken der EU zur Vorbereitung auf schwerwiegende Cybersicherheitsvorfälle und Cybersicherheitsvorfälle großen Ausmaßes
Externes Personal	Siehe oben

Beschreibung zusätzlicher Aufgaben, die von der ENISA ausgeführt werden sollen:

Beamte und Zeitbedienstete	Verwaltung der EU-Cybersicherheitsreserve (Ländermanager und Unterstützung bei der Umsetzung, während die tatsächlichen Betriebskosten der Reserve gemäß dem Cybersolidaritätsgesetz gedeckt werden) (10) Management der einheitlichen Meldeplattform im Rahmen der Cyberresilienzverordnung (Betrieb) (9) Schwachstellenmanagementdienste im Zusammenhang mit der einheitlichen Meldeplattform (4) Ausweitung der einheitlichen Meldeplattform auf die zentrale Anlaufstelle (Entwicklung und Betrieb) (8) Entwicklung von technischen Leitlinien, Sachkenntnis im Bereich Produktsicherheit und Marktanalyse zur Unterstützung der Umsetzung der Cyberresilienzverordnung (7) Normung zur Unterstützung der Umsetzung der Cyberresilienzverordnung / Zertifizierung / NIS 2 (4) Unterstützung der Marktüberwachungstätigkeiten im Rahmen der Cyberresilienzverordnung (4) Unterstützung von Konformitätsprüfungen und Sicherheitsbewertungen von Produkten (4) Unterstützung der Mitgliedstaaten bei der Amtshilfe (3) Bereitstellung von Schwachstellenmanagementdiensten, Aufrechterhaltung der EUVD und Bereitstellung von Beratungs- und anreichernden Funktionen (CVD) (15) Operative Zusammenarbeit und Lageerfassung – Risikominderungs- und Unterstützungsplattformen wie CNW/CyCLONe; Unterstützung der Aufgaben im Zusammenhang mit Warnmeldungen; Unterstützung der verstärkten Koordinierung mit anderen einschlägigen Einrichtungen bei der Entwicklung von Ablagen verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen (Artikel 11 Absatz 1a CSA2) (5) Unterstützung der Resilienz kritischer Sektoren (einschließlich der Umsetzung des Aktionsplans für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern) (4) Entwicklung eines Systems zur Bescheinigung von Kompetenzen (2) Pflege und Überwachung des Systems zur Bescheinigung von Kompetenzen (6) Administrative Tätigkeiten (Rechnungsführer für Gebühren/Personal/IT) (8) Pflege von Zertifizierungssystemen (11) Horizontale Aufgaben – verstärkte Einbeziehung der Interessenträger, Ausarbeitung technischer Spezifikationen und Beteiligung an Normungstätigkeiten zur Unterstützung von Systemen (1)
Externes Personal	Siehe oben Zwei obligatorische ANS pro Mitgliedstaat, die die Tätigkeiten der Agentur unterstützen und als nationale Verbindungsbeamte fungieren, wobei der Schwerpunkt auf der operativen Zusammenarbeit und der koordinierten Offenlegung von Schwachstellen liegt. (13) Die übrigen 27 ANS sollen kostenlos sein und haben daher keine Auswirkungen auf den Haushalt.

Zusätzliche Betriebskosten für die ENISA pro Jahr (2028-2034):

Kosten	Mittelaus	Zeitplan	Erläuterung

	stattung		
Website zu Cybersicherheitskompetenzen	750 000 EUR	50 % im Jahr 2029 50 % im Jahr 2030	Um die Transparenz der Verfahren zu gewährleisten, sieht der Vorschlag vor, dass die ENISA eine Website mit ECFS-Profilen, Bescheinigungssystemen, Informationen über Gebühren für jedes System, empfohlenen Gebühren für jede Bescheinigung und der Liste der befugter Bescheinigungsanbieter unterhält.
Koordinierte Offenlegung von Schwachstellen (CVD)	1 Mio. EUR	Ab 2028	Die Sicherheit von Produkten und Dienstleistungen, die in unserer kritischen Infrastruktur verwendet werden, hängt in hohem Maße davon ab, ob Informationen über festgestellte Schwachstellen und dazu, wie diese behoben werden können, rechtzeitig weitergegeben werden.
Erkenntnisse über Cyberbedrohungen	3 Mio. EUR	Ab 2028	Für den Aufbau eines Lagebilds in Zusammenarbeit zwischen der ENISA und der Kommission.
Zentrale Anlaufstelle	8 Mio. EUR	6 Mio. EUR im Jahr 2028	Um den Digital-Omnibus-Vorschlag der

		500 000 EUR im Jahr 2029 500 000 EUR im Jahr 2030 500 000 EUR im Jahr 2031 500 000 EUR im Jahr 2032	Kommission zur Vereinfachung der Einhaltung der Pflichten zur Meldung von Cybersicherheitsvorfällen und Datenschutzverletzungen durch die Entwicklung und Pflege einer zentralen Anlaufstelle umsetzen zu können.
Pflege der einheitlichen Meldeplattform im Rahmen der Cyberresilienzverordnung u. a.	3 Mio. EUR	Ab 2028	Die von den gemeinsamen Gesetzgebern eingeführte einheitliche Meldeplattform ist das größte IT-System, die jemals in der Geschichte der ENISA entwickelt wurde, und eine tragende Säule der Cyberresilienzverordnung. Die Einrichtung wird derzeit über eine Beitragsvereinbarung finanziert, ihre laufende Verwaltung erfordert jedoch VZÄ (siehe oben) sowie operative Mittel. Der ENISA kommt eine Schlüsselrolle zu, wenn es darum geht, den Erfolg des Unionsrahmens für die Produktsicherheit, der Cyberresilienzverordnung

			dnung, sicherzustellen.
Sichere Kommunikation und Cybersicherheitsreife der ENISA	2 Mio. EUR +	1,1 Mio. EUR Investitionen im Jahr 2028 (CyCLONe/CSIRTs-Plattformen + sichere Kommunikation) 1 Mio. EUR pro Jahr ab 2029 für die Systempflege 1,5 Mio. EUR für die Cybersicherheitsreife	Gewährleistung der Cybersicherheit der Agentur und Kommunikationsinstrumente.
Aufrechterhaltung der Cybersicherheitszertifizierung	1 400 000 Mio. EUR	600 000 EUR im Jahr 2028 1 000 000 EUR im Jahr 2029 1 200 000 EUR im Jahr 2030 1 400 000 EUR im Jahr 2031 1 400 000 EUR im Jahr 2032 1 400 000 EUR im Jahr 2033 1 400 000 EUR im Jahr 2034	Gedeckt durch Gebühren (ab 2032 vollständig)
Systeme zur Bescheinigung der Cybersicherheit	212 920 EUR	Ab 2030 zu 50 % durch den EU-Haushalt gedeckt	Ab 2033 vollständig durch Gebühren gedeckt

3.2.5. Einschätzung der Auswirkungen auf die Investitionen im Zusammenhang mit digitalen Technologien

Obligatorisch: In die Tabelle unten ist die bestmögliche Einschätzung der für den Vorschlag/die Initiative erforderlichen Investitionen in digitale Technologien einzutragen.

Wenn dies für die Durchführung des Vorschlags/der Initiative erforderlich ist, sollten die Mittel unter Rubrik 4 ausnahmsweise in der dafür vorgesehenen Haushaltslinie ausgewiesen werden.

Die unter die Rubriken 1 bis 3 fallenden Mittel sollten als „IT-Ausgaben zur Politikunterstützung für operationelle Programme“ aufgeführt werden. Diese Ausgaben beziehen sich auf die operativen Mittel, die für die Wiederverwendung/den Erwerb/die Entwicklung von IT-Plattformen/Instrumenten verwendet werden, welche in direktem Zusammenhang mit der Durchführung der Initiative und den damit verbundenen Investitionen stehen (z. B. Lizenzen, Studien, Datenspeicherung usw.). Die in dieser Tabelle dargelegten Informationen sollten mit den Angaben in Abschnitt 4 „Digitale Aspekte“ vereinbar sein.

Mittel INSGESAMT für Digitales und IT	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**MFR 2028-2034 INSGESAMT**
RUBRIK 4								
IT-Ausgaben (intern)	0	0	0	0	0	0	0	**0**
Zwischensumme RUBRIK 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Außerhalb der RUBRIK 4								
IT-Ausgaben zur Politikunterstützung für operationelle Programme	0	0	0	0	0	0	0	**0**
Zwischensumme außerhalb der RUBRIK 4	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
INSGESAMT	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

3.2.6. Vereinbarkeit mit dem derzeitigen Mehrjährigen Finanzrahmen

Der Vorschlag/Die Initiative

– ☒ kann durch Umschichtungen innerhalb der entsprechenden Rubrik des Mehrjährigen Finanzrahmens (MFR) in voller Höhe finanziert werden.

Unbeschadet der Verhandlungen über den nächsten MFR werden die der Agentur ab 2028 zugewiesenen Mittel durch Umschichtungen aus Programmen im Rahmen des

MFR 2028-2034 ausgeglichen. Wird eine Ausgleichskürzung erforderlich, müssen die der Agentur zugewiesenen Mittel und ihre Finanzierungsströme und -quellen möglicherweise überprüft werden.

– ☐ erfordert die Inanspruchnahme des verbleibenden Spielraums unter der einschlägigen Rubrik des MFR und/oder den Einsatz der besonderen Instrumente im Sinne der MFR-Verordnung.

– ☐ erfordert eine Änderung des MFR.

3.2.7. Beiträge Dritter

Der Vorschlag/Die Initiative

– ☒ sieht keine Kofinanzierung durch Dritte vor.

– ☐ sieht folgende Kofinanzierung durch Dritte vor:

Mittel in Mio. EUR (3 Dezimalstellen)

	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Insgesamt
Kofinanzierende Einrichtung					
Kofinanzierung INSGESAMT					

3.2.8. Schätzung des Personal- und Mittelbedarfs in einer dezentralen Agentur

Zusätzlicher Personalbedarf (Vollzeitäquivalente)

Agentur: ENISA	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**
Bedienstete auf Zeit (AD-Besoldungsgruppen)	5	11	17	19	19	19	19
Bedienstete auf Zeit (AST-Besoldungsgruppen)	4	7	11	12	12	12	12
Zwischensumme Bedienstete auf Zeit (AD+AST)	***9***	***18***	***28***	***31***	***31***	***31***	***31***
Vertragsbedienstete	22	44	66	74	74	74	74
Abgeordnete nationale Sachverständige	4	8	11	13	13	13	13
Zwischensumme Vertragsbedienstete plus Abgeordnete nationale Sachverständige	26	52	77	87	87	87	87
Personal INSGESAMT	35	70	105	118	118	118	118

Durch einen Beitrag aus dem EU-Haushalt gedeckte Mittel in Mio. EUR (3 Dezimalstellen)

Agentur: ENISA	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**2028-2034 INSGESAMT**

Titel 1: Personalausgaben	4,488	8,466	12,507	13,648	10,584	10,012	9,537	**87,766**
Titel 2: Infrastruktur- und Betriebsausgaben								
Titel 3: Operative Ausgaben	16,413	11,588	11,528	11,788	11,613	11,613	11,113	**85,240**
Aus dem EU-Haushalt gedeckte Mittel INSGESAMT	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**

Etwaige durch Gebühren gedeckte Zahlungen in Mio. EUR (3 Dezimalstellen)

Agentur: ENISA	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**2028-2034 INSGESAMT**
Titel 1: Personalausgaben		0,510	1,043	1,539	4,604	5,176	5,650	**18,522**
Titel 2: Infrastruktur- und Betriebsausgaben								**0,000**
Titel 3: Operative Ausgaben								**0,000**
Durch Gebühren gedeckte Mittel INSGESAMT	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Überblick/Zusammenfassung des Bedarfs an Personal und Mitteln (in Mio. EUR) für den Vorschlag/die Initiative in einer dezentralen Agentur

Agentur: ENISA	Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**	**2028-2034 INSGESAMT**
Bedienstete auf Zeit (AD+AST)	9	18	28	31	31	31	31	*31*
Vertragsbedienstete	22	44	66	74	74	74	74	74
Abgeordnete nationale Sachverständige	4	8	11	13	13	13	13	13
Personal insgesamt	35	70	105	118	118	118	118	**118**
Aus dem EU-Haushalt gedeckte Mittel	**20,901**	**20,054**	**24,035**	**25,437**	**22,197**	**21,625**	**21,151**	**155,4**
Durch Gebühren gedeckte Zahlungen (falls zutreffend)	**0,000**	**0,510**	**1,043**	**1,539**	**4,604**	**5,176**	**5,650**	**18,522**

Kofinanzierte Mittel (falls zutreffend)	0,000	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**
Mittel INSGESAMT	**20,901**	**20,564**	**25,078**	**26,976**	**26,801**	**26,801**	**26,801**	**173,922**

3.3. Geschätzte Auswirkungen auf die Einnahmen

– ☒ Der Vorschlag/Die Initiative wirkt sich nicht auf die Einnahmen aus.

– ☐ Der Vorschlag/Die Initiative wirkt sich auf die Einnahmen aus, und zwar

  – ☐ auf die Eigenmittel

  – ☐ auf die übrigen Einnahmen

  – ☐ Bitte geben Sie an, ob die Einnahmen bestimmten Ausgabenlinien zugeordnet sind.

in Mio. EUR (3 Dezimalstellen)

Einnahmenlinie:	Für das laufende Haushaltsjahr zur Verfügung stehende Mittel	Auswirkungen des Vorschlags/der Initiative[105]						
		Jahr **2028**	Jahr **2029**	Jahr **2030**	Jahr **2031**	Jahr **2032**	Jahr **2033**	Jahr **2034**
Artikel ….								

Bitte geben Sie für die sonstigen zweckgebundenen Einnahmen die betreffende(n) Ausgabenlinie(n) im Haushaltsplan an.

Sonstige Anmerkungen (bei der Ermittlung der Auswirkungen auf die Einnahmen verwendete Methode/Formel oder weitere Informationen).

Die Gebührenmechanismen stehen in Verbindung mit drei Tätigkeitsbereichen der ENISA:

– Gebühren in Verbindung mit der Erteilung der Befugnis an Anbieter im Rahmen der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen.

Die Gebühren in Verbindung mit dieser Tätigkeit werden nach der Annahme der überarbeiteten Cybersicherheitsverordnung in einem Durchführungsrechtsakt festgelegt. Um jedoch den Investitionsbedarf und die entsprechenden Kosten abschätzen zu können, wurden Berechnungen anhand eines bestehenden Modells in einem EU-Mitgliedstaat durchgeführt[106]. Das Modell umfasst einmalige Zahlung und eine jährliche Gebühr.

Festkosten: 8 540 EUR

105 Bei den traditionellen Eigenmitteln (Zölle, Zuckerabgaben) sind die Beträge netto, d. h. abzüglich 20 % für Erhebungskosten, anzugeben.

106 Decision RR-02: *Price list of SNAS services*: https://www.snas.sk/storage/app/uploads/public/677/e79/e4c/677e79e4cac62903312474.pdf,

Jährliche Gebühr: 800 EUR

Mit den Gebühren sollen die Kosten für diese spezifische Tätigkeit refinanziert werden. Die Kosten wurden für einen Zeitraum von fünf Jahren auf 1 064 600 EUR geschätzt. Die spezifischen Kosten der in diesem Betrag enthaltenen Tätigkeiten stehen im Zusammenhang mit der Entwicklung und Pflege von Systemen, einschließlich der Ausgaben der Mitglieder einer Ad-hoc-Arbeitsgruppe, die die ENISA bei der Entwicklung der Systeme unterstützen würde (Kostenerstattung und Bezahlung von Berichterstattern), Dienstreisen zu Anbietern von Vor-Ort-Prüfungen und Fortbildungen für Prüfer, um eine einheitliche Anwendung der Systeme zu gewährleisten:

a) Die Kosten für die Ad-hoc-Arbeitsgruppe würden sich auf 800 000 EUR belaufen,

b) die Ausbildung von zwei Prüfern pro Mitgliedstaat würde sich auf 129 600 EUR belaufen,

c) die Prüfung einer Einrichtung pro Mitgliedstaat würde sich auf 135 000 EUR belaufen.

(a + b + c) / 5 = 212 920 EUR Kosten pro Jahr

Der Vorschlag sah einen Übergangszeitraum und Anfangsinvestitionen in den ersten drei Jahren vor. Während des Übergangszeitraums werden die Kosten aus dem EU-Haushalt gedeckt, in den Jahren 4 und 5 werden 50 % der Kosten gedeckt, in den Jahren 6 und 7 erfolgt die umfassende Anwendung von Gebühren.

Jahr	Gebühren
2028	0
2029	0
2030	0
2031	106 460 (Einnahmen)
2032	106 460 (Einnahmen)
2033	212 920 (Einnahmen)
2034	212 920 (Einnahmen)

– Gebühren in Verbindung mit der Deckung der Kosten für die Pflege eines Systems für die Cybersicherheitszertifizierung, das innerhalb des europäischen Rahmens für die Cybersicherheitszertifizierung (ECCF) angenommen wurde.

Die Gebühren in Verbindung mit dieser Tätigkeit werden nach der Annahme der überarbeiteten Cybersicherheitsverordnung in einem Durchführungsrechtsakt festgelegt. Die Schätzungen der Kosten für die Pflege eines Systems beruhen auf Marktanalysen, die in der Folgenabschätzung zum Vorschlag für die Überarbeitung des Rechtsakts zur Cybersicherheit enthalten sind. Die Gesamtkosten der Tätigkeit für einen Zeitraum von fünf Jahren werden auf 5 600 000 EUR für Betriebskosten und 7 100 000 EUR für VZÄ veranschlagt.

Die jährlichen Kosten für Pflegetätigkeiten werden auf der Grundlage der derzeitigen Erfahrung mit 200 000 EUR pro Jahr der Pflege eines Systems[107] und zwei VZÄ für solche Tätigkeiten (bei jährlichen Kosten von 125 887 EUR pro VZÄ) veranschlagt, wobei das geplante Jahr der Annahme solcher Systeme berücksichtigt wird. Es wird erwartet, dass die Einnahmen aus diesen Gebühren mit der Annahme jedes neuen Systems und der schrittweisen Einführung solcher Systeme steigen werden. Bislang wurde im Rahmen des ECCF ein System (EUCC) angenommen, und die ersten Einnahmen aus der Pflege dieses Systems dürften 2029 fließen. Die Kosten werden voraussichtlich bis 2032 gedeckt.

Die geschätzten Einnahmen wurden unter Zugrundelegung spezifischer Annahmen für jedes mögliche System zu folgenden Aspekten berechnet: erwartete Verbreitung (Zahl der auszustellenden Bescheinigungen), Gültigkeitsdauer jeder Bescheinigung und Zahl der aktiven Konformitätsbewertungsstellen. Es wird erwartet, dass durch die Einführung eines künftigen Systems für die Cyberabwehr erhebliche Einnahmen erzielt werden.

Jahr Einnahmen (Prozentsatz der gedeckten Kosten/Aus dem EU-Haushalt gezahlt)

2028 0

2029 250 000 (11 %/- 1 350 000 EUR) – ein System (EUCC)

2030 783 000 (29 %/- 2 000 000 EUR) – drei Systeme (EUCC, ID-Brieftasche, MSS)

2031 783 000 (25 %/- 1 930 000 EUR) – drei Systeme (EUCC, ID-Brieftasche, MSS)

2032 3 850 000 (122 %/- 2 400 000 EUR) – fünf Systeme (EUCC, ID-Brieftasche, MSS, EUCS, 5G)

2033 4 000 000 (126 %/+ 685 000 EUR) – sechs Systeme (EUCC, ID-Brieftasche, MSS, EUCS, 5G, Cyberabwehr)

2034 4 500 000 (141 %/+ 825 000 EUR) – sieben Systeme

Gebühren in Verbindung mit Testinstrumenten zur Unterstützung von Konformitätsbewertungsverfahren

Die Gebühren in Verbindung mit dieser Tätigkeit werden nach der Annahme der überarbeiteten Cybersicherheitsverordnung in einem Durchführungsrechtsakt festgelegt. Um die geschätzten Kosten und die erwarteten Einnahmen anzugeben, wurden die Berechnungen jedoch auf der Grundlage von Schätzungen der ENISA vorgenommen, die in die Folgenabschätzung zum Vorschlag für die Überarbeitung des Rechtsakts zur Cybersicherheit aufgenommen wurden. Die

[107] Bei der Systempflege werden insbesondere zwei Präsenzsitzungen mit Sachverständigen pro Jahr (100 000 EUR) sowie Kosten für Auftragnehmer, die die Entwicklung und Überprüfung der Begleitunterlagen zum System, die Einführung von Zertifizierungssystemen, die Unterstützung der gegenseitigen Begutachtungen und die Durchführung von Konformitätsbewertungen unterstützen (4 x 15 000 = 60 000 EUR), berücksichtigt. Die Kosten umfassen auch den operativen Teil der CEF-Plattform und der Website der ENISA zur Zertifizierung (40 000 EUR).

Kosten in Verbindung mit der Unterstützung von Test- und Bewertungstätigkeiten werden wie folgt veranschlagt:

VZÄ: 4 pro Jahr

Betriebskosten: 800 000 pro Jahr

Gesamtkosten: 6 500 000 (5 Jahre) Pro Jahr: 1 300 000 EUR

Es wird erwartet, dass für die ENISA im ersten Jahr Anlaufinvestitionen getätigt werden, gefolgt von Systempflegekosten. Diese Kosten würden schrittweise durch Einnahmen aus Gebühren gedeckt.

Jahr	Einnahmen
2028	0
2029	260 000
2030	260 000
2031	650 000
2032	650 000
2033	975 000
2034	975 000

4. DIGITALE ASPEKTE

4.1. Anforderungen von digitaler Relevanz

Allgemeine Beschreibung der Anforderungen von digitaler Relevanz und der damit verbundenen Kategorien (Daten, Digitalisierung und Automatisierung von Prozessen, digitale Lösungen und/oder digitale öffentliche Dienste)

Anforderung	**Beschreibung der Anforderung**	**Von der Anforderung betroffene oder sie betreffende Akteure**	**Verfahren auf übergeordneter Ebene**	**Kategorien**
Artikel 5 Absatz 1 Buchstabe a Unterstützung der Umsetzung des Unionsrechts	a) Unterstützung der Mitgliedstaaten bei der kohärenten Umsetzung der Unionspolitik und des Unionsrecht auf dem Gebiet der Cybersicherheit, auch durch **die Herausgabe technischer Leitlinien und Berichte, die Bereitstellung von Beratung und die Weitergabe bewährter Verfahren sowie durch die Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden in diesem Hinblick**	– ENISA – Mitgliedstaaten	– Verarbeitung von Daten zur Herausgabe technischer Leitlinien und Berichte, Bereitstellung von Beratung und Weitergabe bewährter Verfahren sowie Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden – Erleichterung des Austauschs bewährter Verfahren	Datenverarbeitung Datenfluss
Artikel 5 Absatz 1 Buchstabe b Unterstützung der Umsetzung des Unionsrechts	b) Unterstützung der **Informationsweitergabe in und zwischen Sektoren, vor allem in Bezug auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren** und Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) 2024/2847, **durch die Bereitstellung von bewährten Verfahren und Leitfäden zu den verfügbaren Instrumenten und Verfahren**	– ENISA – in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführte Sektoren – durch die Verordnung (EU) 2024/2847 betroffene Interessenträger	Bereitstellung von bewährten Verfahren und Leitfäden zu den verfügbaren Instrumenten und Verfahren für die Informationsweitergabe	Datenverarbeitung Datenfluss

Artikel 5 Absatz 1 Buchstabe c Unterstützung der Umsetzung des Unionsrechts	c) auf Ersuchen der Kommission Unterstützung der Mitgliedstaaten durch **technische Leitlinien, unter anderem zu Maßnahmen zum Cybersicherheitsrisikomanagement, Instrumenten für die Bewertung des Cybersicherheitsreifegrads und Leitfäden für die Reaktion auf Sicherheitsvorfälle**, die auf die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren zugeschnitten sind, um die Verbesserung des Cybersicherheitsreifegrads und die Einhaltung des Unionsrechts im Bereich der Cybersicherheit zu erleichtern	– EU-Kommission – ENISA – in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführte Sektoren	Bereitstellung technischer Leitlinien	Datenverarbeitung Datenfluss
Artikel 5 Absatz 1 Buchstabe e	e) Unterstützung der Mitgliedstaaten und der einschlägigen Einrichtungen der Union bei der **Entwicklung und Förderung von Strategien im Zusammenhang mit der Cybersicherheit**, die die allgemeine Verfügbarkeit und Integrität des öffentlichen Kerns des offenen Internets bewahren	ENISA Mitgliedstaaten EU-Einrichtungen	Unterstützung bei der Entwicklung und Förderung von Strategien im Zusammenhang mit der Cybersicherheit	Datenverarbeitung Datenfluss
Artikel 5 Absatz 1 Buchstabe f Unterstützung der Umsetzung des Unionsrechts	f) Im Einklang mit der Verordnung (EU) 2024/2847 **Bereitstellung von technischer Beratung und Unterstützung** in Fragen im Zusammenhang mit der Durchführung der genannten Verordnung für die	– ENISA – durch die Verordnung (EU) 2024/2847 betroffene Interessenträger	Die Bereitstellung von technischer Beratung und Unterstützung erfordert die Verarbeitung und Weitergabe von Informationen über regulatorische Anforderungen, Herausforderungen bei der Umsetzung und Leitlinien in Bezug auf die	Datenverarbeitung Datenfluss

	Mitgliedstaaten und die Kommission		Einhaltung der Vorschriften.	
Artikel 5 Absatz 1 Buchstabe h	h) auf Ersuchen des europäischen Datenschutzausschusses Bereitstellung von Beratung zur Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre	ENISA EDSA	Bereitstellung von Beratung auf Ersuchen	Datenverarbeitung Datenfluss
Artikel 5 Absatz 2 Bereitstellung von auf Unionsebene durchgeführten Cybersicherheitsrisikobewertungen	Die ENISA trägt zu auf Unionsebene koordinierten Risikobewertungen in Bezug auf die Cybersicherheit bei, einschließlich der gemäß Artikel 22 der Richtlinie (EU) 2022/2555 durchgeführten Bewertungen.	ENISA Mitgliedstaaten Öffentlichkeit	Beitrag zu koordinierten Risikobewertungen, für die Datenverarbeitung und Datenflüsse erforderlich sind	Datenverarbeitung Datenfluss
Artikel 5 Absatz 3 Die ENISA gibt Leitlinien heraus.	Die ENISA **gibt Leitlinien heraus** für die Interoperabilität der für die Informationsweitergabe verwendeten Netz- und Informationssysteme, auch in Bezug auf grenzübergreifende Cyber-Hubs gemäß Artikel 6 Absatz 3 der Verordnung (EU) 2025/38.	ENISA Mitgliedstaaten	Die ENISA gibt Leitlinien heraus.	Datenverarbeitung Datenfluss

Artikel 5 Absatz 5 Unterstützung der Kommission	Auf **Ersuchen der Kommission stellt die ENISA Sachkenntnis, technische Beratung, Informationen oder Analysen zur Verfügung oder führt vorbereitende Arbeiten zu spezifischen Cybersicherheitsfragen durch**, um die Politikgestaltung der Kommission und die Überwachung der Umsetzung der Rechtsvorschriften der Union zu unterstützen.	EU-Kommission ENISA	Vorbereitung von Informationen und deren Übermittlung an die Kommission	Datenverarbeitung Datenfluss
Artikel 6 Kapazitätsaufbau	Die ENISA stellt Wissen und Sachkenntnis, bewährte Verfahren usw. zur Unterstützung zur Verfügung.	ENISA Mitgliedstaaten EU-Einrichtungen Öffentliche und private Interessenträger Marktüberwachungsbehörden Mitglieder der ECCG ECCC	Bereitstellung von Wissen und Sachkenntnis	Datenverarbeitung Datenfluss
Artikel 7 Sensibilisierung und Talentpool	Die ENISA unterstützt die Mitgliedstaaten bei ihren Bemühungen um die Sensibilisierung für die Politik und die Rechtsvorschriften der Union im Bereich der Cybersicherheit und die Förderung von deren Sichtbarkeit, **indem sie praktisch anwendbare Instrumente und Leitlinien entwickelt**. Die ENISA unterstützt Initiativen zum Ausbau des europäischen Talentpools im Bereich der Cybersicherheit, insbesondere durch die	ENISA Mitgliedstaaten	Entwicklung praktisch anwendbarer Instrumente und Leitlinien	Datenverarbeitung

	Koordinierung von Auswahlverfahren.			
Artikel 8 Absatz 1 Marktkenntnis und -analysen	Die ENISA **führt Analysen** der wichtigsten Markttrends auf dem Cybersicherheitsmarkt sowohl auf der Nachfrage- als auch auf der Angebotsseite **durch**, insbesondere im Zusammenhang mit den Bereichen, in denen europäische Systeme für die Cybersicherheitszertifizierung bestehen oder geplant sind, in den Sektoren gemäß den Anhängen I und II der Richtlinie (EU) 2022/2555 und den unter die Verordnung (EU) 2024/2847, einschließlich der Anhänge III und IV der genannten Verordnung, fallenden Produktkategorien, **und verbreitet diese**.	ENISA in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführte Sektoren durch die Verordnung (EU) 2024/2847 abgedeckte Produktkategorien	Durchführung und Verbreitung von Analysen	Datenverarbeitung Datenfluss
Artikel 8 Absatz 2 Marktkenntnis und -analysen	Die ENISA **führt Analysen** der Trends in der Cybersicherheitstechnik **durch**, insbesondere in Bezug auf Tätigkeiten und Einrichtungen, die in den Anwendungsbereich der Richtlinie (EU) 2022/2555 fallen, und Produkte mit digitalen Elementen, die in den Anwendungsbereich der Verordnung (EU) 2024/2847 fallen, und **verbreitet diese**.	ENISA Öffentlichkeit, Interessenträger im Sinne der Richtlinie (EU) 2022/2555 und der Verordnung (EU) 2024/2847	Durchführung und Verbreitung von Analysen	Datenverarbeitung Datenfluss

Artikel 8 Absatz 3 Marktkenntnis und Unterstützung für Ökosysteme	Die ENISA baut Wissen auf und **verbreitet technische Empfehlungen und Analysen** zu modernsten Instrumenten, Rahmen, Normen und bewährten Verfahren im Bereich der Cybersicherheit.	ENISA Öffentlichkeit	Verbreitung von technischen Empfehlungen und Analysen zu modernsten Instrumenten, Rahmen, Normen und bewährten Verfahren im Bereich der Cybersicherheit.	Datenverarbeitung Datenfluss
Artikel 9 Internationale Zusammenarbeit	Die ENISA leistet einen Beitrag, indem sie die Ergebnisse internationaler Übungen analysiert und dem Verwaltungsrat darüber Bericht erstattet, den Austausch bewährter Verfahren erleichtert und der Kommission Sachkenntnis und Beratung zur Verfügung stellt.	Internationales Publikum ENISA Verwaltungsrat der ENISA EU-Kommission	Analyse und Berichterstattung, Bereitstellung von Beratung usw.	Datenverarbeitung Datenfluss
Artikel 10 Absätze 2 und 3 Operative Zusammenarbeit	2. Die ENISA ist Mitglied des gemäß Artikel 15 Absatz 1 der Richtlinie (EU) 2022/2555 eingerichteten Netzwerks nationaler CSIRTs und n**immt die Sekretariatsgeschäfte** des CSIRTs-Netzwerks gemäß Artikel 15 Absatz 2 der Richtlinie (EU) 2022/2555 **wahr**. 3. Die ENISA **nimmt die Sekretariatsgeschäfte** des Europäischen Netzwerks der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) gemäß Artikel 16 Absatz 2 Unterabsatz 2 der Richtlinie (EU) 2022/2555 **wahr**.	ENISA CSIRTs (Artikel 15 Absatz 1 der Richtlinie (EU) 2022/2555) EU-CyCLONe (Artikel 16 Absatz 2 der Richtlinie (EU) 2022/2555)	Erleichterung des Informationsaustauschs, Wahrnehmung der Aufgaben des Sekretariats der Netzwerke	Datenfluss Digitale Lösung Digitaler öffentlicher Dienst

Artikel 11 Absatz 1 Buchstabe b Lageerfassung Artikel 12 Frühwarnungen	**Ausgabe von Frühwarnungen** im Einklang mit Artikel 12	EU-Kommission ENISA Europol EU-CyCLONe CSIRTs-Netzwerk CERT-EU in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführte Einrichtungen	Ausgabe von Frühwarnungen	Datenverarbeitung Datenfluss Digitaler öffentlicher Dienst
Artikel 10 Absatz 4 Buchstabe b Operative Zusammenarbeit	b) auf Ersuchen eines oder mehrerer Mitgliedstaaten **Bereitstellung von Beratung und Bewertungen in Bezug auf einen bestimmten potenziellen oder andauernden Sicherheitsvorfall bzw. eine entsprechende Cyberbedrohung**, auch durch die Bereitstellung von Sachkenntnis und die **Erleichterung der technischen Bewältigung solcher Vorfälle** sowie durch die **Unterstützung der freiwilligen Weitergabe einschlägiger Informationen und technischer Lösungen zwischen den Mitgliedstaaten**	ENISA Mitgliedstaaten	Bereitstellung von Beratung und Bewertungen in Bezug auf einen bestimmten potenziellen oder andauernden Sicherheitsvorfall bzw. eine entsprechende Cyberbedrohung; Erleichterung der technischen Bewältigung solcher Vorfälle; Unterstützung der freiwilligen Weitergabe einschlägiger Informationen und technischer Lösungen zwischen den Mitgliedstaaten	Datenverarbeitung Datenfluss Digitaler öffentlicher Dienst
Artikel 10 Absatz 4 Buchstabe c Operative Zusammenarbeit	c) Analyse von Schwachstellen, Bedrohungen und Sicherheitsvorfällen	ENISA Mitgliedstaaten	Datenerhebung aus öffentlichen Quellen und Datenaustausch mit den Mitgliedstaaten	Datenverarbeitung Datenfluss

Artikel 10 Absatz 4 Buchstabe d Operative Zusammenarbeit	d) auf **Ersuchen eines oder mehrerer Mitgliedstaaten Unterstützung** in Bezug auf nachträgliche technische Untersuchungen von erheblichen Sicherheitsvorfällen im Sinne der Richtlinie (EU) 2022/2555	ENISA Mitgliedstaaten	Analyse und Unterstützung als Reaktion auf technische Untersuchungen in Verbindung mit Sicherheitsvorfällen	Datenverarbeitung Datenfluss
Artikel 10 Absatz 4 Buchstabe e Operative Zusammenarbeit	e) Beitrag zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene, insbesondere durch **Unterstützung des EU-CyCLONe bei der Erstellung von Berichten an die politische Ebene und durch Erleichterung der zeitnahen Informationsweitergabe zwischen dem CSIRTs-Netzwerk und dem EU-CyCLONe**	ENISA EU-CyCLONe CSIRTs-Netzwerk	Analyse von Daten zur Unterstützung der Ausarbeitung von Berichten; Erleichterung der zeitnahen Informationsweitergabe zwischen Netzwerken	Datenverarbeitung Datenfluss Digitaler öffentlicher Dienst
Artikel 10 Absatz 5 Operative Zusammenarbeit	Auf **Ersuchen eines Mitgliedstaats** oder einer Einrichtung der Union in Zusammenarbeit mit dem CERT-EU unterstützt die ENISA eine kohärente öffentliche Kommunikation über einen Sicherheitsvorfall oder eine Cyberbedrohung.	ENISA Mitgliedstaaten	Empfang des Ersuchens und erforderlichenfalls Kommunikation	Datenfluss

Artikel 10 Absatz 6 Operative Zusammenarbeit	Die ENISA **unterstützt** die Zusammenarbeit zwischen den Mitgliedstaaten und über den CERT-EU zwischen den Einrichtungen der Union im Hinblick auf den **Einsatz sicherer Kommunikationsinstrumente**. Die ENISA verwendet innerhalb des CSIRTs-Netzwerks und des EU-CyCLONe sichere Kommunikationsinstrumente, die von Rechtsträgern bereitgestellt werden, die nicht in Drittländern niedergelassen sind bzw. von Drittländern oder von Staatsangehörigen von Drittländern kontrolliert werden.	ENISA EU-Kommission Mitgliedstaaten EU-Einrichtungen CSIRTs-Netzwerk EU-CyCLONe	Förderung des Einsatzes sicherer Kommunikationsinstrument innerhalb des CSIRTs-Netzwerks und des EU-CyCLONe.	Digitale Lösung Digitaler öffentlicher Dienst
Artikel 11 Absatz 1 Buchstabe a Gemeinsame Lageerfassung im Bereich der Cybersicherheit	a) in Zusammenarbeit mit dem EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission, dem CERT-EU, Europol und anderen einschlägigen Einrichtungen der Union **Entwicklung von Ablagen** verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen, einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren	EU-Kommission ENISA EU-CyCLONe CSIRTs-Netzwerk Europol EU-Einrichtungen CERT-EU	Entwicklung von Ablagen	Digitaler Fluss Digitale Lösung Digitaler öffentlicher Dienst
Artikel 11 Absatz 1 Buchstaben c bis g Gemeinsame Lageerfassung im Bereich der Cybersicherheit	zeitnahe Vorlage von Ad-hoc-Analysen (einige davon auf Ersuchen), Bereitstellung von Analysen und technischer Beratung, Erstellung eines Lageberichts in Zusammenarbeit mit anderen Einrichtungen, Beobachtung und Weitergabe von Trends	ENISA Mitgliedstaaten EU-Kommission EU-Einrichtungen EU-CyCLONe CSIRTs-Netzwerk	Datenanalyse, Informationsweitergabe und Bereitstellung von Berichten (einige davon auf Ersuchen)	Datenverarbeitung Datenfluss

Artikel 11 Absatz 2 Buchstabe a Gemeinsame Lageerfassung im Bereich der Cybersicherheit	Die ENISA **führt Analysen** von Cyberbedrohungen, Sicherheitsvorfällen, Trends, neu aufkommende Technik und ihren Auswirkungen **durch**, einschließlich einer regelmäßigen **Analyse** der in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren und der einschlägigen Produktkategorien, die unter die Verordnung (EU) 2024/2847 fallen.	ENISA Öffentlichkeit	Analyse von Daten zur Bereitstellung von für die Cybersicherheit maßgeblichen Informationen Regelmäßige Berichte	Datenverarbeitung Datenfluss
Artikel 11 Absatz 2 Buchstabe b Gemeinsame Lageerfassung im Bereich der Cybersicherheit	Die ENISA **stellt in Zusammenarbeit mit der Kommission und gegebenenfalls dem CSIRTs-Netzwerk Beratung, Leitlinien und bewährte Verfahren für die Sicherheit der Netz- und Informationssysteme bereit**, vor allem für die Sicherheit der Infrastrukturen, die die in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Sektoren unterstützen.	EU-Kommission CERT-EU CSIRTs-Netzwerk Öffentlichkeit	Bereitstellung von Beratung, Leitlinien und bewährten Verfahren	Datenverarbeitung Datenfluss
Artikel 11 Absatz 2 Buchstabe c Gemeinsame Lageerfassung im Bereich der Cybersicherheit	Die ENISA **führt langfristige strategische Analysen der Cyberbedrohungen und -vorfälle durch**, um neu aufkommende Trends **erkennen** und dazu beitragen zu können, Sicherheitsvorfälle zu vermeiden.	ENISA Öffentlichkeit	Datenanalyse und Erkennung neu aufkommende Trends	Datenverarbeitung

Artikel 11 Absatz 3 Gemeinsame Lageerfassung im Bereich der Cybersicherheit	Die ENISA kann die in Absatz 2 genannten **Analysen**, Ratschläge, Leitlinien, bewährten Verfahren und Berichte im Einvernehmen mit den in Absatz 2 genannten beitragenden Einrichtungen **veröffentlichen**.	ENISA Öffentlichkeit	Veröffentlichung von Informationen	Datenfluss Digitaler öffentlicher Dienst
Artikel 13 Absatz 2 Unterstützung bei der Reaktion auf Sicherheitsvorfälle	2. Auf Ersuchen der Kommission oder des EU-CyCLONe nimmt die ENISA mit Unterstützung des CSIRTs-Netzwerks und mit Zustimmung der betroffenen Mitgliedstaaten eine **Überprüfung und Bewertung schwerwiegender Cybersicherheitsvorfälle** oder von Cybersicherheitsvorfällen großen Ausmaßes im Einklang mit Artikel 21 der Verordnung (EU) 2025/38 vor.	EU-Kommission ENISA EU-CyCLONe CSIRTs-Netzwerk Mitgliedstaaten	Überprüfung und Bewertung schwerwiegender Cybersicherheitsvorfälle	Datenverarbeitung
Artikel 14 Absatz 2 Cybersicherheitsübungen auf Unionsebene	2. Die ENISA **unterhält eine Ablage** der aus den in Absatz 1 genannten Übungen gewonnenen Erkenntnisse und gibt den Mitgliedstaaten und gegebenenfalls den Einrichtungen der Union Empfehlungen dazu, wie die gewonnenen Erkenntnisse wirksam und effizient genutzt werden können.	ENISA Mitgliedstaaten EU-Einrichtungen	Unterhalt einer Ablage	Datenverarbeitung Digitale Lösung Digitaler öffentlicher Dienst
Artikel 14 Cybersicherheitsübungen auf Unionsebene	Auf Ersuchen des EU-CyCLONe, der Kommission, der Mitgliedstaaten oder des CERT-EU organisiert die ENISA Cybersicherheitsübungen oder trägt zu deren Organisation bei. Die ENISA unterstützt die Kommission bei der Erstellung eines jährlichen fortlaufenden Programms von	ENISA Kommission Mitgliedstaaten EU-Einrichtungen CERT-EU	Organisation oder Unterstützung der Organisation von Übungen auf Ersuchen	Datenfluss Datenverarbeitung

	Cybersicherheitsübungen auf Unionsebene.			
Artikel 15 Bereitstellung von Instrumenten und Plattformen	1. **Die ENISA sorgt für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung operativer technischer Instrumente einschließlich Plattformen** für die Cybersicherheit auf Unionsebene, insbesondere der gemäß Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 eingerichteten einheitlichen Meldeplattform zur Meldung von Vorfällen [und der gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstelle], sowie von Testinstrumenten zur Unterstützung der Durchführung von Konformitätsbewertungsverfahren im Einklang mit den einschlägigen Rechtsvorschriften der Union. 2. Soweit angebracht **arbeitet die ENISA** für die Zwecke des Absatzes 1 mit dem CSIRTs-Netzwerk und gegebenenfalls den Marktüberwachungsbehörden **zusammen und tauscht Informationen mit ihnen aus**.	ENISA CSIRTs-Netzwerk Öffentlichkeit Marktüberwachungsbehörden	Die ENISA sorgt für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung operativer technischer Instrumente einschließlich Plattformen.	Digitale Lösung Digitaler öffentlicher Dienst Datenfluss

Artikel 16 Absatz 2 Schwachstellenmanagementdienste	a) Pflege der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank; b) Bereitstellung von Schwachstellenmanagementdiensten für **Interessenträger**, aufbauend auf der europäischen Schwachstellendatenbank und unter Rückgriff auf die der ENISA zur Verfügung stehenden einschlägigen Informationen; c) gegebenenfalls Aufnahme einer strukturierten Zusammenarbeit mit **Organisationen**, die ähnliche Programme, Register oder Datenbanken wie die europäische Schwachstellendatenbank bereitstellen; d) aktive Unterstützung der gemäß Artikel 12 Absatz 1 der Richtlinie (EU) 2022/2555 als Koordinatoren benannten **CSIRTs** im Hinblick auf die Steuerung der koordinierten Offenlegung von Schwachstellen, die erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten nach sich ziehen könnten; e) Entwicklung und Aufrechterhaltung von Methoden und Governance-Mechanismen für die Ermittlung und koordinierte Offenlegung von Schwachstellen **in Zusammenarbeit mit den zuständigen nationalen Behörden, den CSIRTs, der Branche und der Forschungsgemeinschaft**.	ENISA Nationale CSIRTs CSIRTs-Netzwerk Zuständige nationale Behörden Wirtschaft Forschungsgemeinschaft Öffentlichkeit Internationale Akteure, die Programme, Register oder Datenbanken bereitstellen	Bereitstellung von Schwachstellenmanagementdiensten; gegebenenfalls Aufnahme einer strukturierten Zusammenarbeit; Zusammenarbeit mit Interessenträgern	Digitale Lösung Digitaler öffentlicher Dienst Datenfluss

Artikel 17 Cybersicherheitszertifizierung Artikel 18 Normung, technische Spezifikationen und Leitlinien	Artikel 17 Nummer 1 a) **Ausarbeitung möglicher europäischer Systeme für die Cybersicherheitszertifizierung („mögliche Systeme“)** für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und die Cyberabwehr von Einrichtungen und damit verbundener technischer Spezifikationen gemäß Artikel 74; b) **Pflege der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung** gemäß Artikel 75, auch im Hinblick auf eine mögliche Überprüfung der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 76; c) die Förderung der Einführung angenommener Systeme und die Pflege einer eigenen Website mit Informationen über europäische Systeme für die Cybersicherheitszertifizierung, europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen gemäß Artikel 79 und deren Bekanntmachung; Artikel 17 Nummer 2 e) **Ausarbeitung** von Musterbestimmungen, auf die in den	ENISA Öffentlichkeit	Datenanalyse und Austausch von Datenflüssen mit der Kommission und anderen Interessenträgern; Ausarbeitung möglicher Zertifizierungssysteme; Pflege der ENISA-Website	Datenverarbeitung Datenflüsse Digitaler öffentlicher Dienst

	europäischen Systemen für die Cybersicherheitszertifizierung („möglichen Systemen“) von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten und der Cyberabwehr von Einrichtungen gemäß Artikel 81 Absatz 5 Bezug zu nehmen ist. Artikel 18 1. Die ENISA arbeitet technische Spezifikationen und Leitlinien aus, um die Umsetzung der Rechtsvorschriften der Union im Bereich der Cybersicherheit zu unterstützen. 2. Die ENISA **beobachtet die Entwicklung der Normungstätigkeiten** auf Unionsebene und – im Einklang mit Artikel 9 – auf internationaler Ebene, **beteiligt sich gegebenenfalls daran und steuert sie**. 3. Die ENISA unterstützt die Entwicklung und Bewertung kryptografischer Algorithmen. Wird ein kryptografischer Algorithmus positiv bewertet, so arbeitet die ENISA im Einklang mit der Verordnung (EU) Nr. 1025/2012 mit den europäischen Normungsgremien zusammen, um dessen Normung zu unterstützen. 4. Die ENISA **berät** die Kommission und die ECCG **in technischen Fragen** zu geeigneten Normen oder technischen Spezifikationen zur Unterstützung der Unionspolitik im			

	Bereich der Cybersicherheit, insbesondere der Verordnung (EU) 2024/2847, einschließlich der Harmonisierungsrechtsvorschriften der Union im Bereich der Cybersicherheit und der europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 81 Absatz 1 Buchstabe d. 5. Die ENISA unterstützt die Kommission bei der Bewertung der Entwürfe harmonisierter Normen, um die Umsetzung der Harmonisierungsrechtsvorschriften der Union im Bereich der Cybersicherheit zu fördern.			
Artikel 19 – Europäischer Zertifizierungsrahmen für die Cybersicherheit	Die ENISA **entwickelt einen europäischen Kompetenzrahmen für Cybersicherheit („ECSF“) und macht ihn öffentlich zugänglich**. Vor der Veröffentlichung oder Aktualisierung des ECSF gemäß Absatz 4 **konsultiert die ENISA die Kommission**. Die Verwendung des ECSF ist **für öffentliche und private Einrichtungen freiwillig**. Die ENISA kann bei der Entwicklung und Einführung des ECSF **Interessenträger konsultieren**.	ENISA Kommission Öffentlichkeit Mitgliedstaaten EU-Einrichtungen Öffentliche und private Interessenträger	Pflege des ECSF; Konsultation der Interessenträger; Einführung des ECSF	Datenverarbeitung Datenfluss Digitale Lösung
Artikel 20-23 – Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen	Die ENISA ist für die **Entwicklung, Annahme und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen**	ENISA Kommission Öffentlichkeit Mitgliedstaaten	Entwicklung und Pflege von Systemen; Konsultation der Interessenträger; Bearbeitung von Anträgen; Treffen von Entscheidungen; Pflege einer Website	Datenverarbeitung Datenfluss Digitale Lösung

	zuständig. Die Verwendung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen ist **für nationale öffentliche Stellen und private Einrichtungen freiwillig**, sofern im nationalen Recht nichts anderes bestimmt ist. Vor der Einführung eines neuen Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen **konsultiert die ENISA die Kommission**. Die ENISA darf ein solches System erst nach einer befürwortenden **Stellungnahme der Kommission** annehmen. Bei der Ausarbeitung eines Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen kann die ENISA **einschlägige Interessenträger konsultieren**. Die ENISA sorgt während der gesamten Ausarbeitung der Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen für eine **enge Zusammenarbeit mit den Mitgliedstaaten**. Befugte Bescheinigungsanbieter **bewerten, ob Einzelpersonen die Anforderungen** eines Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen **erfüllen**, und stellen, wenn diese Anforderungen erfüllt sind, europäische Einzelbescheinigungen von	EU-Einrichtungen Öffentliche und private Interessenträger (Beitrag zur Entwicklung eines Bescheinigungssystems, Antragsteller und Anbieter europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, einschließlich Prüfer)		Digitaler öffentlicher Dienst

	Cybersicherheitskompetenzen aus. Die ENISA **stellt den Prüfern Orientierungshilfen bereit und führt obligatorische Fortbildungen** für sie zu den Anforderungen und Bewertungsmethoden durch, die in dem in Artikel 20 Absatz 3 Buchstabe b genannten System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen enthalten sind. Einrichtungen, die befugte Bescheinigungsanbieter werden oder ihre Befugnisse erneuern lassen möchten **(„Antragsteller"), stellen einen Antrag** bei der ENISA. Befugte Bescheinigungsanbieter stellen sicher, dass elektronische Einzelbescheinigungen der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen **auf Ersuchen einer Einzelperson** als elektronische Attributsbescheinigungen in einem Format ausgestellt werden, das in den europäischen Brieftaschen für die digitale Identität gemäß der Verordnung (EU) Nr. 910/2014 gespeichert werden kann. Antragsteller und befugte Bescheinigungsanbieter erlauben der **ENISA**, im Rahmen des ursprünglichen Antragsverfahrens, der Aufrechterhaltung der Befugnis oder deren Erneuerung **Bewertungen durchzuführen** und alle			

	einschlägigen Informationen weiterzugeben, um sicherzustellen, dass die in den Absätzen 3 und 4 festgelegten Anforderungen und die in Absatz 5 festgelegten Verpflichtungen gemäß Artikel 22 Absatz 2 (weiterhin) erfüllt werden. Befugte Bescheinigungsanbieter **unterrichten die ENISA** unverzüglich, wenn die in Absatz 3 aufgeführten Anforderungen nicht mehr erfüllt werden oder wenn Zweifel an der Erfüllung dieser Anforderungen bestehen, auch in Bezug auf die Unabhängigkeit der Prüfer. Die Antragsteller **entrichten** für die Bewertung ihres Antrags **eine Gebühr an die ENISA**. Befugte Bescheinigungsanbieter **zahlen eine Gebühr** für die Aufrechterhaltung ihrer Befugnis **an die ENISA**. **Die ENISA bewertet**, ob die in Artikel 21 Absätze 3 und 4 festgelegten Anforderungen und die in Artikel 21 Absatz 5 festgelegten Verpflichtungen von Antragstellern und befugten Bescheinigungsanbietern (weiterhin) erfüllt werden. Nach der Prüfung des Antrags anhand der Anforderungen gemäß Artikel 21 Absätze 3 und 4 **kann die ENISA eine Entscheidung treffen**. **Die ENISA kann solche Entscheidungen ändern, aussetzen oder**			

	widerrufen. **Die ENISA unterhält und aktualisiert regelmäßig eine eigene Website** mit öffentlichen Informationen über a) den ECSF, einschließlich des Rahmens und des Zeitplans für die Aktualisierung; b) die Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, deren Fortschritte und Zeitpläne für die weitere Entwicklung; c) die Gebühren im Zusammenhang mit jedem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, das gemäß Artikel 47 dieser Verordnung			

	angenommen wird; d) die voraussichtlichen Kosten einer europäischen Einzelbescheinigung von Cybersicherheitskompetenzen gemäß Artikel 20 Absatz 4; e) die Liste befugter Bescheinigungsanbieter.			
Artikel 25 Zusammensetzung des Verwaltungsrats	**Ernennung der Mitglieder** des Verwaltungsrats der ENISA	ENISA EU-Kommission Mitgliedstaaten	Ernennung von Mitgliedern	Datenfluss Datenverarbeitung
Artikel 28 Absatz 1 Aufgaben des Verwaltungsrats Artikel 30 Exekutivrat	b. Annahme des Entwurfs des in Artikel 44 genannten einheitlichen Programmplanungsdokuments der ENISA an, bevor dieser **der Kommission zur Stellungnahme vorgelegt wird**; f) **Bewertung** und Annahme des konsolidierten Jahresbericht über die Tätigkeiten der ENISA, einschließlich des Jahresabschlusses und der Ausführungen darüber, inwiefern die ENISA die vorgegebenen Leistungsindikatoren erfüllt hat, und **Übermittlung des**	ENISA EU-Kommission Europäisches Parlament Rat der EU Rechnungshof Mitgliedstaaten Öffentlichkeit	Übermittlung des einheitlichen Programmplanungsdokument an die Kommission zur Stellungnahme; Bewertung und Annahme des konsolidierten Jahresbericht über die Tätigkeiten der ENISA, einschließlich des Jahresabschlusses und der Ausführungen darüber, inwiefern die ENISA die vorgegebenen Leistungsindikatoren erfüllt hat, und Übermittlung des Jahresberichts und der Bewertung; Folgemaßnahmen zu den Feststellungen	Datenfluss Datenverarbeitung

	Jahresberichts und der Bewertung bis zum 1. Juli des folgenden Jahres an das Europäische Parlament, den Rat, die Kommission und den Europäischen Rechnungshof; Veröffentlichung des Jahresberichts; i) Sicherstellung geeigneter **Folgemaßnahmen zu den Feststellungen** und Empfehlungen, die sich aus den internen oder externen Prüfberichten und Bewertungen sowie aus den Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und der Europäischen Staatsanwaltschaft (EUStA) ergeben			
Artikel 31 Absatz 8 Ernennung und Abberufung sowie Verlängerung der Amtszeit	Der **Verwaltungsrat unterrichtet das Europäische Parlament** über seine Absicht, die Amtszeit des Exekutivdirektors im Einklang mit Absatz 6 zu verlängern. Innerhalb von drei Monaten vor der Verlängerung der Amtszeit gibt der Exekutivdirektor, sofern er dazu aufgefordert wird, vor dem zuständigen Ausschuss des Europäischen Parlaments eine Erklärung ab und beantwortet Fragen der Mitglieder.	ENISA Verwaltungsrat der ENISA Europäisches Parlament	Der Verwaltungsrat unterrichtet das Europäische Parlament.	Datenfluss

Artikel 32 Absatz 3 Aufgaben und Zuständigkeiten des Exekutivdirektors Artikel 32 Absatz 5	3. Der **Exekutivdirektor erstattet dem Europäischen Parlament** über die Wahrnehmung seiner Aufgaben **Bericht**, wenn er dazu aufgefordert wird. Der Rat kann den Exekutivdirektor auffordern, über diese Tätigkeit Bericht zu erstatten. Ausarbeitung von Haushaltsplanentwürfen, Strategien und Strategiedokumenten.	Exekutivdirektor der ENISA Europäisches Parlament	Berichterstattung über die Leistung	Datenfluss Datenverarbeitung
Artikel 35 Absätze 5 und 6 ENISA-Beratungsgruppe	5. Die ENISA-Beratungsgruppe **berät die ENISA** bei der Durchführung ihrer Aufgaben, ausgenommen der Anwendung der Bestimmungen der Titel III, IV und V dieser Verordnung. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Jahresarbeitsprogramms der ENISA und bei der Kommunikation mit den einschlägigen Interessenträgern in Bezug auf Fragen im Zusammenhang mit dem Jahresarbeitsprogramm. 6. Die ENISA-Beratungsgruppe **unterrichtet den Verwaltungsrat** regelmäßig über ihre Tätigkeiten.	ENISA Mitglieder der ENISA-Beratungsgruppe Verwaltungsrat der ENISA Exekutivdirektor der ENISA	Beratung und Information über ihre Tätigkeiten	Datenverarbeitung Datenfluss
Artikel 36-43 Beschwerdekammer	Die ENISA **richtet eine Beschwerdekammer** durch einen Beschluss des Verwaltungsrats ein. Die Beschwerdekammer besteht aus einem Vorsitzenden und drei weiteren Mitgliedern. Jedes Mitglied der Beschwerdekammer hat einen Stellvertreter. Der Stellvertreter vertritt	ENISA Verwaltungsrat der ENISA Kommission Beschwerdekammer im Sinne von Artikel 36 des CSA2-Vorschlags Antragsteller (juristische	Treffen von Entscheidungen auf der Grundlage von Beschwerden Bearbeitung von Beschwerden Ausarbeitung und Veröffentlichung der Geschäftsordnung Informationsströme	Datenverarbeitung Datenfluss Digitaler öffentlicher Dienst

	das Mitglied in dessen Abwesenheit. Der **Vorsitzende, die weiteren Mitglieder und ihre Stellvertreter** werden vom Verwaltungsrat **anhand einer von der Kommission festgelegten Liste qualifizierter Kandidaten ernannt**. Die Liste der qualifizierten Kandidaten gilt vier Jahre lang. Die Gültigkeit der Liste kann auf Vorschlag der Kommission vom Verwaltungsrat um jeweils vier Jahre verlängert werden. Die Beschwerdekammer kann den **Verwaltungsrat ersuchen, zwei zusätzliche Mitglieder und deren Stellvertreter** von der in Absatz 3 genannten Liste **zu ernennen**, wenn sie der Ansicht ist, dass die Art der Beschwerde dies erfordert. Die Beschwerdekammer **gibt sich eine Geschäftsordnung und veröffentlicht diese**. Ist ein Mitglied einer Beschwerdekammer aus einem der in Absatz 1 aufgeführten Gründe oder aus einem sonstigen Grund der Ansicht, an einem Beschwerdeverfahren nicht mitwirken zu können, so **teilt es dies der Beschwerdekammer mit**. Die Beschwerdekammer **entscheidet über das Vorgehen** in den Fällen der Absätze 2 und 3 ohne Mitwirkung des betreffenden Mitglieds. Das betreffende Mitglied wird bei diesem Beschluss durch seinen Stellvertreter in der	Personen, die befugte Bescheinigungsanbieter werden, ihre Befugnis aufrechterhalten oder verlängern lassen wollen)		

	Beschwerdekammer vertreten. Eine gemäß Absatz 1 eingelegte Beschwerde unterliegt einem Abhilfeverfahren gemäß Artikel 41, bevor sie der Beschwerdekammer zur Prüfung vorgelegt wird. Beschwerdeführer im Sinne des Artikels 21 Absatz 3 können **Rechtsmittel einlegen gegen eine an sie gerichtete Entscheidung der ENISA** gemäß Artikel 22 Absatz 3, die Versäumnis der ENISA, innerhalb der in Artikel 22 Absatz 4 festgelegten geltenden Fristen in Bezug auf den von ihnen eingereichten Antrag tätig zu werden. In dem in Absatz 1 Buchstabe a genannten Fall ist die Beschwerde zusammen mit einer Begründung gemäß Artikel 36 Absatz 5 innerhalb von zwei Monaten nach Bekanntgabe der Entscheidung an den betreffenden Beschwerdeführer oder, falls keine Bekanntgabe erfolgt ist, innerhalb von zwei Monaten ab dem Zeitpunkt, zu dem der Beschwerdeführer von der Entscheidung Kenntnis erlangt hat, **schriftlich einzulegen**. In dem in Absatz 1 Buchstabe b genannten Fall ist die Beschwerde gemäß der in Artikel 36 Absatz 5 genannten Geschäftsordnung innerhalb von zwei Monaten nach Ablauf der in Artikel 22 Absatz 4 genannten Frist **schriftlich bei**			

	der ENISA einzulegen. Erachtet die ENISA die Beschwerde als zulässig und begründet, so **korrigiert sie die Entscheidung oder die Untätigkeit** gemäß Artikel 40 Absatz 1. Wird die Entscheidung nicht innerhalb eines Monats nach Eingang der Beschwerde von der ENISA korrigiert, so **entscheidet die ENISA umgehend, ob sie den Vollzug ihrer Entscheidung aussetzt, und legt die Beschwerde der Beschwerdekammer vor**. Die **Beschwerdekammer entscheidet** innerhalb von drei Monaten nach Einreichung einer Beschwerde, ob sie dieser stattgibt oder sie zurückweist. Bei der Prüfung einer Beschwerde wird die Beschwerdekammer innerhalb der in ihrer Geschäftsordnung festgelegten Fristen tätig. Sie **fordert die am Beschwerdeverfahren Beteiligten** so oft wie erforderlich **auf, innerhalb bestimmter Fristen Stellungnahmen zu ihren Bescheiden oder zu den Schriftsätzen der anderen Beteiligten des Beschwerdeverfahrens einzureichen**. Die am Beschwerdeverfahren Beteiligten haben das Recht, **mündliche Erklärungen** abzugeben. Stellt die Beschwerdekammer fest, dass die Beschwerde begründet ist, **verweist sie die Angelegenheit an die ENISA zurück**. Die ENISA **trifft ihre**			

	endgültige Entscheidung in Übereinstimmung mit den Feststellungen der Beschwerdekammer und **begründet diese Entscheidung**. Die ENISA **unterrichtet die Beteiligten** des Beschwerdeverfahrens hierüber. Klagen zur Aufhebung von Entscheidungen der ENISA, die gemäß Artikel 22 Absatz 3 getroffen wurden, oder Klagen wegen Untätigkeit gemäß Artikel 22 Absatz 4 können **beim Gerichtshof der Europäischen Union erhoben werden**, nachdem das in den Artikeln 39 bis 42 vorgesehene Beschwerdeverfahren innerhalb der ENISA ausgeschöpft wurde, oder bei Untätigkeit innerhalb der geltenden Frist gemäß Artikel 41 Absatz 2. Die ENISA hat **alle erforderlichen Maßnahmen zu ergreifen**, um dem Urteil des Gerichtshofs der Europäischen Union nachzukommen.			
Artikel 44 Einheitliches Programmplanungsdokument	2. Jedes Jahr erstellt der Exekutivdirektor einen Entwurf des in Absatz 1 genannten einheitlichen Programmplanungsdokuments und der entsprechenden Finanz- und Personalplanung nach Artikel 32 der Delegierten Verordnung (EU) 2019/715 der Kommission und unter Berücksichtigung der von der Kommission festgelegten Leitlinien. 3. Bis zum 30. November eines jeden Jahres nimmt der Verwaltungsrat das in	Exekutivdirektor der ENISA Verwaltungsrat der ENISA EU-Kommission Europäisches Parlament Rat	Jährliche Ausarbeitung, Annahme und Übermittlung eines einheitlichen Programmplanungsdokuments	Datenfluss

	Absatz 1 genannte einheitliche Programmplanungsdokument an, wobei er die Stellungnahme der Kommission nach Artikel 32 Absatz 7 der Delegierten Verordnung (EU) 2019/715 der Kommission berücksichtigt. Wenn der Verwaltungsrat beschließt, Teile der Stellungnahme der Kommission nicht zu berücksichtigen, legt er eine ausführliche Begründung für diesen Beschluss vor. Der Verwaltungsrat leitet das einheitliche Programmplanungsdokument bis zum 31. Januar des Folgejahres sowie jede spätere Aktualisierung dieses Dokuments an das Europäische Parlament, den Rat und die Kommission weiter.			
Artikel 45 Aufstellung des Haushaltsplans der ENISA	4. Die **Kommission übermittelt den Entwurf des Voranschlags** zusammen mit dem Entwurf des Gesamthaushaltsplans der Union **der Haushaltsbehörde**. Der Entwurf des Voranschlags wird auch der ENISA zur Verfügung gestellt.	ENISA EU-Kommission	Informationsweitergabe	Datenfluss
Artikel 47 Gebühren	Für jede Tätigkeit im Rahmen des Systems europäischer Bescheinigungen gemäß Artikel 22 Absatz 1 werden zulasten von Antragstellern im Sinne des Artikels 21 Absatz 3 oder von befugten Bescheinigungsanbietern als Beitrag zur vollständigen Deckung der Kosten der von der ENISA durchgeführten Tätigkeiten **folgende Gebühren erhoben**:	Kommission ENISA Bescheinigungsanbieter Konformitätsbewertungsstellen	Verarbeitung von Informationen; Zahlung von Gebühren; Berichterstattung über Gebühren	Datenverarbeitung Datenfluss

	a. Erteilung von Befugnissen nach Prüfung der in Artikel 21 Absätze 3 und 4 festgelegten Anforderungen, einschließlich der Durchführung von Bewertungen; b. jährliche Aufrechterhaltung der Befugnis; c. Erneuerung der Befugnis für Anbieter europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, einschließlich der Durchführung von Bewertungen. Im Zusammenhang mit der Zertifizierung werden **zulasten der Konformitätsbewertungsstellen** für die Pflege der europäischen Systeme für die Cybersicherheitszertifizierung, in deren Rahmen europäische Cybersicherheitszertifikate ausgestellt werden, insbesondere **folgende Gebühren erhoben**: eine jährliche Gebühr für die Teilnahme an einem europäischen System für die Cybersicherheitszertifizierung; eine Gebühr für die Ausstellung europäischer Cybersicherheitszertifikate im Rahmen europäischer Systeme für die Cybersicherheitszertifizierung. Die unter Buchstabe b genannten Gebühren werden erhoben, wenn die Konformitätsbewertungsstelle der ENISA europäische Cybersicherheitszertifikate			

	zur Veröffentlichung auf ihrer Website gemäß Artikel 79 übermittelt. Die **Kommission erlässt Durchführungsrechtsakte** mit Durchführungsbestimmungen, die für die von der ENISA erhobenen Gebühren gelten. Die ENISA legt im Rahmen des Rechnungslegungsverfahrens **einen Bericht über die erhobenen Gebühren und deren Einfluss auf ihren Haushalt** vor.			
Artikel 48 Artikel 49 Auswirkungen auf den Haushalt	Artikel 48 3. Jedes Jahr **übermittelt** der Exekutivdirektor **der Haushaltsbehörde alle Informationen**, die für die Ergebnisse von Bewertungsverfahren von Belang sind. Artikel 49 1. Bis zum 1. März des jeweils folgenden Haushaltsjahres (1. März des Jahres n + 1) **übermittelt** der Rechnungsführer der ENISA dem Rechnungsführer der Kommission und dem Rechnungshof **den vorläufigen Jahresabschluss für das Haushaltsjahr** (Jahr n). 2. Der Rechnungsführer der ENISA **übermittelt dem Rechnungsführer der Kommission** auf die von Letzterem vorgeschriebene Weise bzw. in dem von ihm vorgeschriebenen Format auch **die erforderlichen Rechnungsführungsinformationen zu**	ENISA Verwaltungsrat der ENISA EU-Kommission Rat Europäisches Parlament	Verarbeitung und Weitergabe von Informationen in Bezug auf den Haushalt der ENISA	Datenverarbeitung Datenfluss

	Konsolidierungszwecken bis zum 1. März des Jahres N + 1. 3. **Die ENISA übermittelt dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof den Bericht über die Haushaltsführung und das Finanzmanagement** für das Jahr N bis zum 31. März des Jahres N + 1. 4. **Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Rechnungsabschluss der ENISA für das Jahr N**, erstellt der Rechnungsführer der ENISA in eigener Verantwortung den endgültigen Jahresabschluss der ENISA. 5. Der **Verwaltungsrat gibt eine Stellungnahme** zum endgültigen Rechnungsabschluss der ENISA für das Jahr N **ab**. **Der Rechnungsführer der Agentur erstellt in eigener Verantwortung den endgültigen Jahresabschluss der ENISA. Der Exekutivdirektor legt ihn dem Verwaltungsrat zur Stellungnahme vor.**			

Artikel 52 Interessenerklärung	Die Beteiligten **geben eine Verpflichtungserklärung und eine Interessenerklärung ab, aus der hervorgeht, ob direkte oder indirekte Interessen bestehen**, die ihre Unabhängigkeit beeinträchtigen könnten.	ENISA-Verwaltung (Exekutivdirektor, stellvertretender Exekutivdirektor), Verwaltungsrat, abgeordnete nationale Sachverständige	Verarbeitung und Weitergabe von Daten zur Interessenerklärung	Datenverarbeitung Datenfluss
Artikel 58 Verbindungsbeamte	1. **Jeder Mitgliedstaat benennt** gemäß Artikel 59 Absatz 2 **mindestens zwei Verbindungsbeamte** [von seiner nationalen Cybersicherheitsbehörde] als zur ENISA abgeordnete nationale Sachverständige, die an ihrem Sitz oder ihrer Außenstelle tätig sind. Die Kommission kann ebenfalls einen Verbindungsbeamten benennen. 2. Von ihrem Mitgliedstaat benannte Verbindungsbeamte sind dazu befugt, nach strikter Maßgabe des nationalen Rechts oder der nationalen Gepflogenheiten ihres jeweiligen Mitgliedstaats, insbesondere in Bezug auf Datenschutz und Vertraulichkeit, **alle einschlägigen Informationen**, wie von dieser Verordnung vorgesehen, **von ihrem jeweiligen Mitgliedstaat anzufordern und zu erhalten**.	ENISA Mitgliedstaaten	Benennung von Verbindungsbeamten und Informationsweitergabe	Datenverarbeitung Datenfluss

Artikel 67 Umgang mit Verschlusssachen	Nach **Konsultation der Kommission** legt die ENISA die Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von nicht als Verschlusssachen eingestuften vertraulichen Informationen und von EU-Verschlusssachen enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443 und 2015/444 festgelegt sind. Die Sicherheitsvorschriften der ENISA enthalten **Bestimmungen über den Austausch, die Verarbeitung und die Speicherung derartiger Informationen**.	ENISA Verwaltungsrat Kommission	Umgang mit Verschlusssachen	Datenverarbeitung Datenfluss
Artikel 68, 69, 70 Zusammenarbeit mit Einrichtungen der Union und nationalen Behörden Zusammenarbeit mit Interessenträgern Zusammenarbeit mit Drittländern	Die ENISA arbeitet mit den einschlägigen Einrichtungen der Union, den Marktüberwachungs- und Aufsichtsbehörden, einschlägigen Interessenträgern, zuständigen Behörden aus Drittländern oder internationalen Organisationen zusammen und tauscht Informationen mit ihnen aus.	ENISA Europol ECCC Europäischer Datenschutzausschuss Öffentlichkeit Rat	Informationsweitergabe	Datenfluss

Artikel 72 zu öffentlichen Informationen und Konsultationen über die europäischen Systeme für die Cybersicherheitszertifizierung	2. Die Kommission unterhält eine eigene Website mit Informationen zu den folgenden Aspekten und aktualisiert diese regelmäßig: a) europäische Systeme für die Cybersicherheitszertifizierung, deren Entwicklung in Auftrag gegeben wurde; b) strategische Prioritäten für die Harmonisierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder Sicherheitsanforderungen des Unionsrechts, einschließlich möglicher Bereiche, für die ein europäisches System für die Cybersicherheitszertifizierung in Auftrag gegeben werden könnte. 3. Die Kommission macht auf der in Absatz 2 genannten Website die Informationen über ihre Beauftragung der ENISA mit der Ausarbeitung eines möglichen Systems gemäß Artikel 73 und über ihren Beschluss, ein von der ENISA gemäß Artikel 74 Absatz 7 übermitteltes mögliches System anzunehmen, abzulehnen oder einzustellen, öffentlich zugänglich.	EU-Kommission Öffentlichkeit ENISA	Pflege der Informationswebsite Damit wird die Kommission bevollmächtigt, Informationen auf einer öffentlich zugänglichen Website bereitzustellen und fortlaufend entsprechende Datenverwaltungstätigkeiten durchzuführen.	Digitale öffentliche Dienste Digitale Lösung
Artikel 72 zu öffentlichen Informationen und Konsultationen über die europäischen Systeme für die Cybersicherheitszertifizierung	Während der Ausarbeitung eines möglichen Systems durch die ENISA gemäß Artikel 74 **können das Europäische Parlament und der Rat die Kommission** in ihrer Eigenschaft als Vorsitzende der ECCG und die ENISA **ersuchen**, einschlägige Informationen über den Entwurf eines möglichen	ENISA Rat der EU Europäisches Parlament	Ersuchen um und Übermittlung von Informationen über einen von der ENISA ausgearbeiteten Entwurf eines möglichen Systems	Datenflüsse

	Systems vorzulegen. **Auf Ersuchen des Europäischen Parlaments oder des Rates kann die ENISA im Einvernehmen mit der Kommission** und unbeschadet des Artikels 54 **dem Europäischen Parlament und dem Rat relevante Teile des Entwurfs eines möglichen Systems** in einer dem erforderlichen Vertraulichkeitsniveau angemessenen Weise und gegebenenfalls in eingeschränkter Form **zur Verfügung stellen**. **Das Europäische Parlament und der Rat können die Kommission und die ENISA ersuchen, Angelegenheiten zu erörtern**, die die Umsetzung der europäischen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen betreffen.			
Artikel 73 Aufträge für ein europäisches System für die Cybersicherheitszertifizierung Artikel 74 Ausarbeitung und Annahme europäischer Systeme für die Cybersicherheitszertifizierung **(fällt unter Artikel 17)**	**Artikel 73** **1. Die Kommission kann die ENISA beauftragen, ein mögliches System für die Cybersicherheitszertifizierung** für IKT-Produkte, -Dienste oder -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen **auszuarbeiten**. In hinreichend begründeten Fällen kann die ECCG der Kommission vorschlagen, einen Auftrag gemäß Absatz 1 zu erteilen.	EU-Kommission ENISA ECCG Fachkundige Interessenträger	Ausarbeitung eines Auftrags und eines Zertifizierungssystems und entsprechende Konsultation der Interessenträger	Datenverarbeitung Datenflüsse Digitale öffentliche Dienste (fällt unter Artikel 17)

	4. Bei der Ausarbeitung des in Absatz 1 genannten Auftrags konsultiert **die Kommission** die ENISA und die ECCG ordnungsgemäß und berücksichtigt die Standpunkte aller **einschlägigen Interessenträger** und anderer Einrichtungen der Union, gegebenenfalls einschließlich derjenigen, die nach den Rechtsvorschriften der Union relevant sind, nach denen ein europäisches System für die Cybersicherheitszertifizierung eine Konformitätsvermutung begründet. Artikel 74 3. Bei der Ausarbeitung des möglichen Systems **arbeitet** die ENISA **eng mit der ECCG zusammen**. Die **ECCG leistet der ENISA Unterstützung** und fachliche Beratung bei der Ausarbeitung des möglichen Systems und gegebenenfalls unterstützender technischer Spezifikationen. **Die ENISA ersucht die Mitglieder der ECCG um schriftliche Stellungnahmen zu dem möglichen System.** 4. **Die ENISA konsultiert die Interessenträger** zeitnah im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses. **Die ENISA arbeitet außerdem mit den**			

	zuständigen Behörden in den Mitgliedstaaten und mit den einschlägigen Einrichtungen der Union zusammen, um deren fachliche Beratung zur Ausarbeitung des möglichen Systems und gegebenenfalls einer unterstützenden technischen Spezifikation **einzuholen**. 6. **Die ENISA übermittelt** der Kommission **das mögliche System** spätestens 60 Tage nach dem Datum des in Absatz 5 genannten Auftrags. 7. Bei Erhalt des möglichen **Systems bewertet die Kommission**, ob das System dem Auftrag gemäß Artikel 73 entspricht. 8. Verweist die Kommission ein mögliches System gemäß Absatz 7 Buchstabe b zur Überarbeitung zurück an die ENISA, so gelten die Absätze 4, 5 und 7 entsprechend.			
Artikel 75 Pflege eines europäischen Systems für die Cybersicherheitszertifizierung	2. Die ENISA stellt – in Zusammenarbeit mit der Kommission und mit Unterstützung der ECCG und ihrer einschlägigen für die Systempflege zuständigen Untergruppe – die Pflege des europäischen Systems für die Cybersicherheitszertifizierung sicher, auch im Hinblick auf die mögliche Überprüfung solcher Systeme durch die Kommission. Die ENISA arbeitet mit den einschlägigen Einrichtungen der Union und Gruppen in Verbindung mit	EU-Kommission ENISA ECCG Konformitätsbewertungsstellen	Die ENISA sorgt für die Systempflege. Dazu gehören regelmäßige Hybrid- oder Online-Sitzungen, die Sammlung, Analyse und Weitergabe von Informationen (im Zusammenhang mit einem europäischen System für die Cybersicherheitszertifizierung)	Datenverarbeitung Datenfluss

	Systempflegetätigkeiten zusammen und tauscht Informationen mit ihnen aus. 5. Die ECCG kann eine Stellungnahme zur Pflege europäischer Systeme für die Cybersicherheitszertifizierung abgeben.			
Artikel 76 Bewertung, Überprüfung und Widerruf eines europäischen Systems für die Cybersicherheitszertifizierung	1. Mindestens alle vier Jahre nach dem Beginn der Anwendung eines europäischen Systems für die Cybersicherheitszertifizierung bewertet die ENISA in Zusammenarbeit mit der für die Systempflege zuständigen Untergruppe der ECCG und unter Berücksichtigung der Rückmeldungen der Interessenträger die Wirkung und die Wirksamkeit dieses Systems. Die ENISA nimmt eine Bewertung vor, indem sie die erforderliche Marktanalyse im Einklang mit Artikel 8 Absatz 1 durchführt. 3. Bei der Überprüfung oder dem Widerruf europäischer Systeme für die Cybersicherheitszertifizierung konsultiert die Kommission die ENISA, die ECCG und ihre einschlägige für die Systempflege zuständige Untergruppe und trägt darüber hinaus den Standpunkten der einschlägigen Interessenträger und anderer Einrichtungen der Union Rechnung. 4. Die ECCG kann eine Stellungnahme zur Überprüfung oder zum Widerruf eines europäische Systems für die Cybersicherheitszertifizierung abgeben.	EU-Kommission ENISA ECCG	Die Kommission überprüft die Systeme unter Einbeziehung der einschlägigen Interessenträger.	Datenverarbeitung Datenfluss

	Die Kommission trägt dieser Stellungnahme bei der Überprüfung oder dem Widerruf des europäischen Systems für die Cybersicherheitszertifizierung gebührend Rechnung.			
Artikel 77 Technische Spezifikationen in europäischen Systemen für die Cybersicherheitszertifizierung	3. Wird in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 auf technische Spezifikationen Bezug genommen, so werden diese auf der in Artikel 79 genannten Website öffentlich zugänglich gemacht. 4. In hinreichend begründeten Fällen, insbesondere wenn die technischen Spezifikationen Informationen enthalten, die die Sicherheit zertifizierter IKT-Produkte, -Dienste und -Prozesse, verwalteter Sicherheitsdienste oder die Cyberabwehr von Einrichtungen gefährden könnten, werden sie nur an die Interessenträger weitergegeben, die von den Anforderungen des Systems betroffen sind. Auf solche Systeme für die Cybersicherheitszertifizierung darf nicht gemäß Artikel 74 Absatz 10 Bezug genommen werden.	ENISA Mitgliedstaaten Konformitätsbewertungsstellen	Bereitstellung von Informationen auf der Zertifizierungswebsite der ENISA	Datenfluss Digitale öffentliche Dienste
Artikel 79 Website zu europäischen Schemata für die Cybersicherheitszertifizierung	1. Die ENISA organisiert Tätigkeiten zur Förderung der Einführung angenommener europäischer Systeme für die Cybersicherheitszertifizierung, unter anderem durch Pflege der in Absatz 2 genannten Website.	ENISA Mitgliedstaaten Konformitätsbewertungsstellen	Im Zuge der Pflege der Informationswebsite wird die ENISA bevollmächtigt, Zertifizierungsinformationen zu sammeln, zu verarbeiten und sie in umfassende Datenbanken einzupflegen, was laufende Datenverwaltungstätigkeiten erfordert.	Digitale öffentliche Dienste Digitale Lösung Datenverarbeitung Datenfluss

	2. Die ENISA unterhält eine eigene Website mit öffentlichen Informationen zu Folgendem und aktualisiert diese regelmäßig: a) europäische Systeme für die Cybersicherheitszertifizierung; b) die mit der Pflege jedes europäischen Systems für die Cybersicherheitszertifizierung verbundenen Gebühren; c) einschlägigen technischen Spezifikationen der ENISA; d) europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, einschließlich Informationen in Bezug auf solche Zertifikate und Erklärungen, die nicht mehr gültig sind, ausgesetzt oder widerrufen wurden oder abgelaufen sind; e) einschlägige zusätzliche Cybersicherheitsinformationen im Einklang mit Artikel 84 Absatz 2; f) Zusammenfassungen gegenseitiger Begutachtungen gemäß Artikel 89 Absatz 7; g) technischen Spezifikationen, auf die in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 Bezug genommen wird. 3. Gegebenenfalls werden **auf der Website gemäß Absatz 2 auch** die nationalen Cybersicherheitszertifizierungssysteme			

	angegeben, die durch ein europäisches System für die Cybersicherheitszertifizierung ersetzt wurden.			
Artikel 81 Elemente europäischer Systeme für die Cybersicherheitszertifizierung	5. Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung gemeinsamer Grundsätze und Musterbestimmungen für die in den Absätzen 1, 2 und 3 genannten Elemente aller europäischen Systeme für die Cybersicherheitszertifizierung zu erlassen. Soweit angemessen und verfügbar, kann ein europäisches System für die Cybersicherheitszertifizierung Verweise auf diese Grundsätze und Musterbestimmungen enthalten. Die in Absatz 5 genannten Durchführungsrechtsakte werden gemäß dem Prüfverfahren nach Artikel 118 Absatz 2 erlassen. **Bei der Entwicklung oder Überarbeitung der gemeinsamen Grundsätze und Musterbestimmungen für die Elemente europäischer Systeme für die Cybersicherheitszertifizierung konsultiert die Kommission die ENISA und berücksichtigt gegebenenfalls die Standpunkte der ECCG, einschlägiger Interessenträger und anderer einschlägiger Stellen.**	ENISA Öffentlichkeit Behörden der Mitgliedstaaten	Konsultation einschlägiger Interessenträger, die Datenflüsse und -verarbeitung erfordert	Datenfluss Datenverarbeitung
Artikel 83 Selbstbewertung der Konformität	3. Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder	ENISA Öffentlichkeit Behörden der Mitgliedstaaten	Zur Verfügung stehende Informationen, Datenweitergabe Weitergegebene Daten erfordert Verarbeitung durch die ENISA und	Datenfluss Datenverarbeitung

	die Einrichtung, deren Cyberabwehr Gegenstand einer Zertifizierung ist, hält die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, -Dienste oder -Prozesse, verwalteten Sicherheitsdienste oder der Cyberabwehr mit dem europäischen System für die Cybersicherheitszertifizierung während des Zeitraums, der in dem entsprechenden System festgelegt ist, für die gemäß Artikel 89 benannte nationale Behörde für die Cybersicherheitszertifizierung bereit. **Eine Kopie der EU-Konformitätserklärung ist der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA unverzüglich vorzulegen.**		Behörden der Mitgliedstaaten	
Artikel 84 Ergänzende Informationen über die Cybersicherheit zertifizierter IKT-Produkte, -Dienste und -Prozesse	1. Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, für die eine EU-Konformitätserklärung oder eine europäisches Cybersicherheitszertifikat ausgestellt wurde, **macht ergänzende Cybersicherheitsangaben öffentlich zugänglich**.	Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen Öffentlichkeit Konformitätsbewertungsstellen	Informationen werden in elektronischer Form öffentlich zugänglich gemacht.	Datenfluss
Artikel 85 Ausstellung europäischer Cybersicherheitszertifikate	2. Die in Artikel 91 genannten Konformitätsbewertungsstellen stellen ein europäisches Cybersicherheitszertifikat auf der Grundlage der Kriterien des nach Artikel 74 angenommenen europäischen Systems für die	ENISA Öffentlichkeit Behörden der Mitgliedstaaten Konformitätsbewertungsstellen	Weitergabe von für Zertifizierungsprozesse relevanten Informationen	Datenfluss Datenverarbeitung

	Cybersicherheitszertifizierung aus. 6. Die natürliche oder juristische Person, die ihre IKT-Produkte, -Dienste oder -Prozesse, oder verwalteten Sicherheitsdienste zur Zertifizierung einreicht, oder die Einrichtung, die einen Antrag auf Zertifizierung ihrer Cyberabwehr stellt, hat der gemäß Artikel 89 benannten **nationalen Behörde für die Cybersicherheitszertifizierung** –sofern diese Behörde die Stelle ist, die das europäische Cybersicherheitszertifikat ausstellt – oder der in Artikel 91 genannten Konformitätsbewertungsstelle **alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen**. 7. Konformitätsbewertungsstellen und gegebenenfalls nationale **Behörden** für die Cybersicherheitszertifizierung **unterrichten die ENISA** unverzüglich über ihre Entscheidungen, die sich auf den Status der europäischen Cybersicherheitszertifikate und der EU-Konformitätserklärung im Einklang mit Artikel 94 auswirken. 8. **Der Inhaber eines europäischen Cybersicherheitszertifikats unterrichtet die Konformitätsbewertungsstelle** und gegebenenfalls die nationale Behörde für die Cybersicherheitszertifizierung gemäß Absatz 7 über etwaige später festgestellte Schwachstellen oder Unregelmäßigkeiten			

	hinsichtlich des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses, des verwalteten Sicherheitsdienstes oder der Cyberabwehr einer Einrichtung, die sich wahrscheinlich auf die Konformität mit Zertifikat auswirken. **Diese Stelle leitet diese Informationen unverzüglich** an die betreffende nationale Behörde für die Cybersicherheitszertifizierung **weiter** und bewertet die Auswirkungen auf das Zertifikat im Einklang mit den Bedingungen des Systems gemäß Artikel 81 Buchstabe f.			
Artikel 86 Nationale Systeme für die Cybersicherheitszertifizierung	4. **Die Mitgliedstaaten unterrichten die Kommission und die ECCG, bevor sie neue nationale Systeme für die Cybersicherheitszertifizierung** von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten und der Cyberabwehr von Einrichtungen **annehmen**.	ENISA Mitgliedstaaten EU-Kommission	Informationsweitergabe	Datenfluss
Artikel 88 Nationale Behörden für die Cybersicherheitszertifizierung	2. Jeder Mitgliedstaat **teilt der Kommission den Namen der benannten nationalen Behörden für die Cybersicherheitszertifizierung mit**. Sofern ein Mitgliedstaat mehr als eine Behörde benennt, teilt er der Kommission auch die Aufgaben mit, die diesen Behörden jeweils zugewiesen wurden. 6. Die nationalen Behörden für die Cybersicherheitszertifizierung haben folgende Aufgaben: c) **in Zusammenarbeit mit den zuständigen**	ENISA Behörden der Mitgliedstaaten EU-Kommission Öffentlichkeit Konformitätsbewertungsstellen	Die Mitgliedstaaten übermitteln der Kommission die benannten nationalen Behörden für die Cybersicherheitszertifizierung. Die Behörden der Mitgliedstaaten nehmen verschiedene Überwachungs-, Aufsichts- und Kooperationsaufgaben wahr, für die Datenflüsse und Datenverarbeitung erforderlich sind.	Datenfluss Datenverarbeitung

	Marktüberwachungsbehörden Überwachung der Einhaltung und Durchsetzung der in dieser Verordnung festgelegten Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen **Hersteller oder Anbieter** von IKT-Produkten, -Diensten oder -Prozessen, verwalteten Sicherheitsdiensten oder Einrichtungen, deren Cyberabwehr zertifiziert wird, die eine Selbstbewertung der Konformität in dem entsprechenden europäischen System für die Cybersicherheitszertifizierung durchführen; d) unbeschadet des Artikels 91 Absatz 3 **aktive Unterstützung der nationalen Akkreditierungsstellen oder anderen einschlägigen Behörden bei der Überwachung und Beaufsichtigung** der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung; e) Zusammenarbeit mit der Europäischen Kommission, wenn die Zuständigkeit einer Konformitätsbewertungsstelle gemäß Artikel 94 angefochten wird; f) **Überwachung und Beaufsichtigung der Tätigkeiten** der in Artikel 85 Absatz 3 genannten öffentlichen Stellen; g) gegebenenfalls Zulassung der Konformitätsbewertungsstellen nach			

	Artikel 93, Überwachung der Befolgung der Vorschriften und Durchsetzung der Pflichten der Konformitätsbewertungsstellen zusammen mit den in den europäischen Systemen für die Cybersicherheitszertifizierung gemäß Artikel 81 Absatz 3 Buchstabe f festgelegten zusätzlichen oder spezifischen Anforderungen und Beschränkung, Aussetzung oder Widerruf bestehender Zulassungen, wenn die Konformitätsbewertungsstellen gegen die Anforderungen dieser Verordnung verstoßen; h) **Bearbeitung von Beschwerden**, die von natürlichen oder juristischen Personen in Bezug auf europäische Cybersicherheitszertifikate, die von der nationalen Behörde für die Cybersicherheitszertifizierung ausgestellt wurden, oder in Bezug auf europäische Cybersicherheitszertifikate, die [nach Artikel 85 Absatz 4] von Konformitätsbewertungsstellen ausgestellt wurden, oder in Bezug auf EU-Konformitätserklärungen nach Artikel 83 eingereicht werden, Untersuchung des Beschwerdegegenstands in angemessenem Umfang und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;			

	i) jährliche Übermittlung eines Jahresberichts über ihre Haupttätigkeiten an die Kommission, die ENISA und die ECCG bis jeweils zum 31. März [Jahr des Inkrafttretens + 12 Monate] und Bereitstellung dieser Berichte für das Begutachtungsteam, wenn die nationale Behörde für die Cybersicherheitszertifizierung einer gegenseitigen Begutachtung gemäß Artikel 89 unterliegt; j) **Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung**, Marktüberwachungsbehörden oder anderen Behörden; dies beinhaltet auch die Weitergabe von Informationen über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten sowie der Cyberabwehr von Einrichtungen mit den Anforderungen dieser Verordnung oder mit den Anforderungen bestimmter europäischer Systeme für die Cybersicherheitszertifizierung; k) **Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung**. 8. Die nationalen Behörden für die Cybersicherheitszertifizierung arbeiten untereinander und mit der Kommission zusammen, indem sie insbesondere **Informationen, Erfahrungen und**			

	bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten sowie die Cyberabwehr von Einrichtungen **austauschen**. 9. Bis zum [6 Monate nach Inkrafttreten] entwickelt die ENISA in Zusammenarbeit mit der Kommission und der ECCG ein Muster für den in Absatz 6 Buchstabe i genannten Bericht.			
Artikel 89 Gegenseitige Begutachtung	5. In Zusammenarbeit mit der Kommission und der ECCG **unterstützt die ENISA** die Organisation des Mechanismus der gegenseitigen Begutachtung und der gegenseitigen Begutachtungen selbst, unter anderem **durch die Entwicklung einschlägiger Leitlinien und Muster**. 7. Der **Abschlussbericht, einschließlich etwaiger Leitlinien** oder Empfehlungen, und die Zusammenfassung der gegenseitigen Begutachtung werden von der ECCG geprüft, die die Zusammenfassung zur Veröffentlichung auf der in Artikel 79 Absatz 2 genannten Website billigt.	EU ENISA ECCG	Bereitstellung von Daten online	Datenfluss Datenverarbeitung

Artikel 90 Europäische Gruppe für die Cybersicherheitszertifizierung (ECCG)	3. Die Europäische Gruppe für die Cybersicherheitszertifizierung hat folgende Aufgaben: [Verweis auf andere Artikel] h) Sie prüft die einschlägigen Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung, auch auf nationaler Ebene gemäß Artikel 86, und tauscht Informationen und bewährte Verfahren in Bezug auf Cybersicherheitszertifizierungssysteme aus; i) sie erleichtert die Zusammenarbeit zwischen den nationalen Behörden für die Cybersicherheitszertifizierung nach den Vorschriften dieses Titels im Wege des Kapazitätsaufbaus und des Informationsaustauschs, insbesondere in Fragen der Cybersicherheitszertifizierung; [Verweis auf andere Artikel] k) sie erleichtert die Anpassung europäischer Systeme für die Cybersicherheitszertifizierung an international anerkannte Normen, unter anderem im Rahmen der Pflege bestehender europäischer Systeme für die Cybersicherheitszertifizierung, und unterbreitet der ENISA erforderlichenfalls Empfehlungen, sich mit den einschlägigen europäischen oder internationalen Normungsgremien in Verbindung zu setzen, um	Mitgliedstaaten ENISA EU-Kommission	Analyse, Informationsweitergabe und Zusammenarbeit zwischen den Behörden der Mitgliedstaaten und internationalen Organisationen im Zusammenhang mit der europäischen Cybersicherheitszertifizierung	Datenverarbeitung Datenfluss

	Unzulänglichkeiten oder Lücken in verfügbaren europäischen oder international anerkannten Normen anzugehen.			
Artikel 92 Weitere Harmonisierung der Zuständigkeit von Konformitätsbewertungsstellen	4. Wird einer nationalen Behörde für die Cybersicherheitszertifizierung ein Antrag nach Absatz 3 vorgelegt, **informiert sie die nationale Behörde für die Cybersicherheitszertifizierung des Mitgliedstaates, in dem die beantragende Konformitätsbewertungsstelle niedergelassen ist**. In solchen Fällen kann die nationale Behörde für die Cybersicherheitszertifizierung dieses Mitgliedstaats als Beobachterin an dem Zulassungsverfahren teilnehmen.	Behörden der Mitgliedstaaten Konformitätsbewertungsstellen	Informationsweitergabe und -aufbewahrung	Datenfluss Datenverarbeitung
Artikel 93 Notifizierung von Konformitätsbewertungsstellen	1. Für jedes europäische System für die Cybersicherheitszertifizierung notifizieren die nationalen **Behörden** für die Cybersicherheitszertifizierung **eines Mitgliedstaats der Kommission und den anderen Mitgliedstaaten** die Konformitätsbewertungsstellen, die akkreditiert und gegebenenfalls nach Artikel 92 zugelassen wurden. 2. **Die nationalen Behörden für die Cybersicherheitszertifizierung führen die Notifizierung** gemäß Absatz 1 mithilfe des von der Kommission entwickelten und verwalteten elektronischen Notifizierungsinstruments **durch**.	ENISA Mitgliedstaaten EU-Kommission Konformitätsbewertungsstellen	Notifizierung akkreditierter und befugter Konformitätsbewertungsstellen	Datenflüsse Datenverarbeitung

Artikel 94 Anfechtung der Zuständigkeit von Konformitätsbewertungsstellen	1. 1. **Die Kommission untersucht** alle Fälle, in denen sie die Kompetenz einer Konformitätsbewertungsstelle in Bezug auf die Erfüllung oder die dauerhafte Erfüllung der für die Stelle geltenden Anforderungen und die Wahrnehmung der entsprechenden Zuständigkeiten durch eine Konformitätsbewertungsstelle anzweifelt oder ihr Zweifel daran zur Kenntnis gebracht werden. 2. **Die nationale Behörde für die Cybersicherheitszertifizierung erteilt der Kommission** auf Verlangen sämtliche Auskünfte über die Grundlage für die Notifizierung oder die Aufrechterhaltung der Zuständigkeit der Konformitätsbewertungsstelle. 3. **Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen erlangten sensiblen Informationen vertraulich behandelt werden.** 4. Stellt die Kommission fest, dass eine Konformitätsbewertungsstelle die Voraussetzungen für ihre Notifizierung nicht oder nicht mehr erfüllt, **setzt sie die nationale Behörde für die Cybersicherheitszertifizierung davon in Kenntnis** und fordert diese auf, die erforderlichen Korrekturmaßnahmen zu treffen, einschließlich eines Widerrufs der Notifizierung, sofern dies nötig ist.	Kommission Mitgliedstaaten ENISA	Anfechtung der Zuständigkeit von Konformitätsbewertungsstellen	Datenfluss Datenverarbeitung Digitaler öffentlicher Dienst
Artikel 95 Verpflichtung von	1. Die Konformitätsbewertungsstellen **unterrichten die nationale Behörde für**	Behörden der Mitgliedstaaten	Informationsaustausch der Konformitätsbewertungsstellen	Datenfluss Datenverarbeitung

Konformitätsbewertungsstellen zur Bereitstellung und Aufbewahrung von Informationen	**die Cybersicherheitszertifizierung** über Folgendes: a) alle Verweigerungen, Einschränkungen, Aussetzungen und Widerrufe einer Bescheinigung oder eines Zertifikats; b) alle Umstände mit Auswirkungen auf den Anwendungsbereich und die Bedingungen der Notifizierung gemäß Artikel 93 Absatz 1; c) alle Auskunftsersuchen über Konformitätsbewertungstätigkeiten, die sie von den Marktüberwachungsbehörden erhalten haben; d) auf Verlangen alle Konformitätsbewertungstätigkeiten, denen sie im Anwendungsbereich ihrer Notifizierung nachgegangen sind, und welche anderen Tätigkeiten, einschließlich grenzübergreifender Tätigkeiten und Vergabe von Unteraufträgen, sie ausgeführt haben. 2. **Die Konformitätsbewertungsstellen stellen der ENISA auch die** in Absatz 1 Buchstabe a genannten **Informationen zur Verfügung**, um ihr die Erfüllung ihrer Aufgabe gemäß Artikel 79 zu erleichtern. 3. Im Rahmen dieser Verordnung **übermitteln Konformitätsbewertungsstellen den**	Konformitätsbewertungsstellen		

	übrigen Konformitätsbewertungsstellen, die ähnliche Konformitätsbewertungstätigkeiten in Bezug auf IKT-Produkte, -Dienste oder -Prozesse, verwaltete Sicherheitsdienste oder Einrichtungen, deren Cyberabwehr zertifiziert wird, nachgehen, unverzüglich **die einschlägigen Informationen** über negative und auf Verlangen auch über positive Ergebnisse von Konformitätsbewertungen. 4. **Konformitätsbewertungsstellen führen ein Aufzeichnungssystem**, das alle Unterlagen und Nachweise enthält, die im Zusammenhang mit jeder von ihnen durchgeführten Bewertung und Zertifizierung erstellt oder entgegengenommen werden. Die Aufzeichnungen werden in sicherer und zugänglicher Weise so lange gespeichert, wie dies für die Zwecke der Zertifizierung erforderlich ist, und mindestens für einen Zeitraum von fünf Jahren nach Ablauf oder Widerruf des jeweiligen europäischen Cybersicherheitszertifikats.			
Artikel 96 Beschwerderecht und Recht auf einen wirksamen	2. Die Behörde oder Stelle, bei der die Beschwerde eingelegt wurde, **unterrichtet den Beschwerdeführer**	Behörden der Mitgliedstaaten EU-Kommission	Informationsfluss in Bezug auf Beschwerden zwischen Behörden und Öffentlichkeit	Datenfluss

gerichtlichen Rechtsbehelf	**über den Stand des Verfahrens** und die getroffene Entscheidung sowie über das Recht auf einen wirksamen gerichtlichen Rechtsbehelf nach den Absätzen 3 und 4. 4. Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats eingeleitet, in dem die Behörde oder Stelle, gegen die der Rechtsbehelf gerichtet ist, ihren Sitz hat.	Öffentlichkeit Inhaber von Zertifikaten	Gerichtsverfahren in den Mitgliedstaaten	
Artikel 97 Sanktionen	**Die Mitgliedstaaten teilen der Kommission** diese Vorschriften und Maßnahmen **unverzüglich mit** und melden ihr alle diesbezüglichen Änderungen.	Behörden der Mitgliedstaaten EU-Kommission	Informationsfluss im Zusammenhang mit Notifizierungen der Mitgliedstaaten an die Kommission über Sanktionen.	Datenfluss
Artikel 99 Sicherheitsrisikobewertungen	Die Kommission oder mindestens drei Mitgliedstaaten können die NIS-Koordinierungsgruppe beauftragen, innerhalb von sechs Monaten koordinierte Risikobewertungen durchzuführen. Die Kommission kann kürzere Fristen fordern. Im Rahmen der Risikobewertungen werden Risikoszenarien entwickelt und wird von Datenanalysen ausgegangen. Vorbereitung koordinierter Sicherheitsrisikobewertungen In Fällen, in denen ein sofortiges Eingreifen gerechtfertigt ist, konsultiert die Kommission unverzüglich die Mitgliedstaaten und führt eine Risikobewertung durch.	EU-Kommission EU-Mitgliedstaaten NIS-Kooperationsgruppe ENISA	Ersuchen um und Empfang von Informationen, Datenanalyse für die Zwecke koordinierter Risikobewertungen Konsultation der Mitgliedstaaten und Durchführung einer Risikobewertung	Datenverarbeitung Datenfluss

	Entscheidungen über die Durchführung von Risikobewertungen (Datenverarbeitung/-analyse).			
Artikel 100 Absätze 1 und 2 zur Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen	1. Wenn sich infolge der Sicherheitsrisikobewertung gemäß Artikel 99 oder anhand anderer Quellen, wie einer öffentlichen Erklärung im Namen der Union oder eines Mitgliedstaats, zeigt, dass von einem Drittland schwerwiegende, strukturelle nicht technische Risiken für die IKT-Lieferketten ausgehen, muss die Kommission die von diesem Land ausgehende Bedrohung unter Berücksichtigung einer Reihe von Elementen überprüfen, die die Verarbeitung/Analyse von Daten zur Folge haben. 2. Gelangt die Kommission nach der in Absatz 1 genannten Überprüfung zu dem Schluss, dass von einem Drittland schwerwiegende und strukturelle nicht technische Risiken für IKT-Lieferketten ausgehen, so kann sie dieses Drittland im Wege eines Durchführungsrechtsakts als Land benennen, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen, die	EU-Mitgliedstaaten EU-Kommission	Empfang, Analyse und Austausch von Informationen	Datenflüsse Datenverarbeitung

	die Verarbeitung/Analyse von Daten und Datenflüsse zur Folge haben.			
Artikel 101 Allgemeiner Mechanismus für die IKT-Lieferketten Artikel 102 Ermittlung wichtiger IKT-Assets Artikel 103 Risikominderungsmaßnahmen in der IKT-Lieferketten	1. Hat die NIS-Kooperationsgruppe eine auf Unionsebene koordinierte Sicherheitsrisikobewertung gemäß Artikel 99 Absätze 1 und 2 dieser Verordnung durchgeführt, oder nach Abschluss des Verfahrens im Falle einer erheblichen Cyberbedrohung gemäß Artikel 99 Absatz 3 kann die Kommission Maßnahmen gemäß den Artikeln 102 und 103 ergreifen. Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, in denen die wichtigen IKT-Assets und Risikominderungsmaßnahmen festgelegt werden, einschließlich Beschränkungen und Verboten im Zusammenhang mit IKT-Lieferketten (Einzelheiten siehe Abschnitt 4.5). Zur Vorbereitung dieses Prozesses berücksichtigt und erwägt die Kommission mehrere Aspekte, die sich auf die **Datenverarbeitung/-analyse und in einigen Fällen auf den Datenfluss beziehen**: Artikel 102 Buchstaben a bis f	EU-Kommission NIS-Kooperationsgruppe Einschlägige Interessenträger	Datenanalyse/Datenverarbeitung, Konsultation einschlägiger Interessenträger	Datenverarbeitung Datenfluss

	Artikel 103 Absatz 4 Buchstaben a bis d Artikel 103 Absatz 6			
Artikel 104 Ermittlung von Hochrisikoanbietern	Die Kommission erstellt im Wege von Durchführungsrechtsakten Listen von Hochrisikoanbietern, für die die mit Durchführungsrechtsakten gemäß Artikel 103 Absatz 1 erlassenen Verbote oder das Verbot gemäß Artikel 111 Absatz 1 relevant sind. Die Kommission erstellt eine Bestandsaufnahme der Anbieter, die IKT-Komponenten und Komponenten, die IKT-Komponenten enthalten, und führt eine Anfangsbewertung durch, um festzustellen, welche Anbieter möglicherweise in gemäß Artikel 100 benannten Drittländern niedergelassen sind oder von solchen Drittländern aus kontrolliert werden. Die Kommission bewertet den Ort der Niederlassung sowie die Eigentums- und Kontrollstruktur. Die Kommission ist berechtigt, die erforderlichen Auskünfte von den Anbietern zu verlangen, teilt dem betreffenden Anbieter die vorläufigen Feststellungen in Bezug auf die	EU-Kommission Zuständige Behörden Anbieter	Datenanalyse/Datenverarbeitung, Konsultation der zuständigen Behörden, Konsultation von Anbietern	Datenverarbeitung Datenfluss

	Niederlassung, die Eigentumsverhältnisse und die Kontrolle des betreffenden Anbieters mit und gibt ihm Gelegenheit, gehört zu werden. Die Kommission kann eine zuständige Behörde ersuchen, die Anfangsbewertung der Niederlassung, Eigentumsverhältnisse und Kontrolle eines Anbieters vorzunehmen, wenn dies angesichts der Merkmale der Tätigkeit dieses Anbieters gerechtfertigt ist. Eine zuständige Behörde kann anbieten, eine solche Anfangsbewertung durchzuführen. Die Kommission überprüft diese ersten Feststellungen, um zu entscheiden, ob der Anbieter in die Liste der Hochrisikoanbieter aufgenommen werden sollte. Die Kommission aktualisiert die Liste der Hochrisikoanbieter regelmäßig, indem sie Hochrisikoanbieter streicht oder hinzufügt. In der Liste aufgeführte Hochrisikoanbieter können die Kommission ersuchen, ihre Niederlassung sowie Kontroll- und Eigentumsstruktur neu zu bewerten, wenn sie nachweisen, dass			

	es relevante Änderungen gegeben hat.			
Artikel 105 Ausnahmen für Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert werden Artikel 108 Vertraulichkeit	1. Eine Einrichtung, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen ist oder die von einem solchen Drittland aus kontrolliert wird, kann bei der Kommission **einen begründeten Antrag auf Ausnahme stellen**. 3. Die Kommission bewertet den Antrag und erlässt einen Beschluss, in dem sie **mehrere Aspekte berücksichtigt**, die eine Datenanalyse zur Folge haben. (Artikel 105 Absätze 3 und 4) Durch die Kommission erlangte Informationen dürfen nur zu dem Zweck verwendet werden, zu dem sie erlangt wurden.	EU-Kommission Einrichtungen, die in einem benannten Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert werden	Eingang des Antrags bei der Kommission, Datenanalyse.	Datenfluss Datenverarbeitung
Artikel 107 Register	Die Kommission führt ein öffentlich zugängliches Register ihrer in Artikel 105 genannten Beschlüsse. Das Register enthält die Namen der Einrichtungen, die Gegenstand solcher Beschlüsse sind.	EU-Kommission Einrichtungen, die in einem benannten Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von einem solchen Drittland aus kontrolliert	Führung eines öffentlich zugänglichen Registers durch die Kommission	Digitale Lösung

		werden		
Artikel 111 Verbote für mobile, feste und satellitengestützte elektronische Kommunikationsnetze	Die gemäß dieser Verordnung benannte zuständige Behörde **unterrichtet** die gemäß der Verordnung (EU) XX/XXXX [DNA-Vorschlag] zuständige Behörde unverzüglich über die Maßnahmen, die Anbietern von mobilen, festen und satellitengestützten elektronischen Kommunikationsnetzen auferlegt wurden.	Zuständige Behörde im Sinne von Artikel 9 oder 20 der Verordnung (EU) XX/XXXX [DNA-Vorschlag] Anbieter mobiler, fester und satellitengestützter elektronischer Kommunikationsnetze	Informationsfluss in Bezug auf Befugnisse von zuständigen Behörden an Einrichtungen	Datenfluss
Artikel 112 Absätze 1 und 4 Zuständige Behörden	1. **Jeder Mitgliedstaat benennt** mindestens eine zuständige Behörde, die für die Aufsichts- und Durchsetzungsaufgaben gemäß Artikel 114 zuständig ist. 4. Die Mitgliedstaaten notifizieren der Kommission unverzüglich die Namen der gemäß Absatz 1 benannten zuständigen Behörden, die jeweiligen Aufgaben dieser Behörden sowie etwaige spätere Änderungen dieser Angaben. Außerdem veröffentlichen die Mitgliedstaaten die Namen der gemäß Nummer 1 benannten zuständigen Behörden.	EU-Mitgliedstaaten EU-Kommission Öffentlichkeit	Benennung der zuständige Behörden und Notifizierung der Kommission durch die Mitgliedstaaten	Datenfluss

Artikel 113 Netz für die Zusammenarbeit und Unterstützungsdienste der Kommission	1. Die Kommission richtet ein Netz für die Zusammenarbeit der zuständigen Behörden der Mitgliedstaaten und der Kommission ein, das als Plattform für die Zusammenarbeit und den Informationsaustausch dient. Die Kommission stellt dem Netz administrative Unterstützung bereit. 2. Um die Mitgliedstaaten bei ihren Aufsichtsaufgaben zu unterstützen, bewertet die Kommission, ob Anbieter, die von bestimmten Verboten betroffen sein könnten, in gemäß Artikel 100 benannten Drittländern, für die Cybersicherheitsbedenken bestehen, niedergelassen sind oder von solchen Drittländern aus kontrolliert werden. Dazu gibt die zuständige Behörde die einschlägigen Informationen an die Kommission weiter. 3. Für die Zwecke der Bewertung ist die Kommission berechtigt, die erforderlichen Auskünfte von Anbietern anzufordern, die von bestimmten Verboten betroffen sein könnten, in gemäß Artikel 100 benannten Drittländern niedergelassen sind oder von solchen Drittländern aus	Kommission Zuständige Behörden Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Art	Bewertung der Anbieter durch die Kommission und Weitergabe der Informationen an zuständige Behörden, die sich mit Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art austauschen Kommission verlangt Informationen von Anbietern Zuständige Behörden unterrichten die Kommission	Datenverarbeitung Datenflüsse

	kontrolliert werden. 4. Nach Abschluss einer Bewertung gibt die Kommission die Feststellungen an die zuständigen Behörden innerhalb des gemäß Nummer 1 eingerichteten Netzes weiter. Die zuständigen Behörden unterrichten die Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Art rechtzeitig von den Feststellungen. 5. Erhält eine zuständige Behörde Kenntnis davon, dass ein Anbieter, der von bestimmten Verboten betroffen sein könnte, in Drittländern, für die Cybersicherheitsbedenken bestehen, niedergelassen ist oder von solchen Drittländern aus kontrolliert wird, und der keiner Bewertung unterzogen wurde, so unterrichtet sie unverzüglich die Kommission davon.			
Artikel 114 Aufsichts- und Durchsetzungsmaßnahmen	Anforderungen an die Mitgliedstaaten, die den Informationsfluss mit den in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Einrichtungen gewährleisten. Bevor sie Maßnahmen ergreifen, teilen die zuständigen Behörden den	EU-Mitgliedstaaten EU-Kommission Einrichtungen gemäß den Anhängen I und II der Richtlinie (EU) 2022/2555	Anforderungen zur Gewährleistung des Informationsflusses,	Datenfluss Datenverarbeitung

	betreffenden Einrichtungen ihre vorläufigen Feststellungen mit. Die zuständigen Behörden kooperieren untereinander und mit der Kommission.			
Artikel 115 Sanktionen	Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.	EU-Kommission EU-Mitgliedstaaten	Mitgliedstaaten, die die Kommission notifizieren	Datenfluss
Artikel 116 Amtshilfe	Wenn eine in Anhang I oder II der Richtlinie (EU) 2022/2555 genannte Einrichtung ihre Dienste in mehr als einem Mitgliedstaat erbringt oder wenn sie ihre Dienste in einem oder mehreren Mitgliedstaaten erbringt und sich ihre wichtigen Assets in einem oder mehreren anderen Mitgliedstaaten befinden, **so arbeiten die zuständigen Behörden der betreffenden Mitgliedstaaten zusammen und unterstützen einander**. Die in Unterabsatz 1 Buchstabe c genannte Amtshilfe kann	EU-Mitgliedstaaten	Amtshilfe bei Aufsichtsmaßnahmen.	Datenfluss Datenverarbeitung

	Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen. Die ersuchte zuständige Behörde darf das Amtshilfeersuchen nur ablehnen, wenn festgestellt wird, dass sie für die erbetene Amtshilfe nicht zuständig ist, dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde steht oder dass das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, deren Offenlegung bzw. Ausführung den wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung des betreffenden Mitgliedstaats zuwiderlaufen würde. Bevor die zuständige Behörde ein solches Ersuchen ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden sowie – auf Ersuchen eines der betreffenden Mitgliedstaaten – die Kommission. Die zuständigen Behörden verschiedener Mitgliedstaaten können gemeinsame Aufsichtsmaßnahmen			

	durchführen, wenn dies angebracht ist und im gegenseitigen Einvernehmen geschieht.			
Artikel 1 Absatz 8, Richtlinie Meldung von Ransomware-Angriffen (Artikel 27 Absatz 13 NIS2)	In Artikel 23 werden folgende Absätze 12 und 13 angefügt: „(13) Die Mitgliedstaaten stellen sicher, dass die betroffenen Einrichtungen im Falle eines erheblichen Sicherheitsvorfalls, der durch einen Ransomware-Angriff verursacht wurde, auf Ersuchen des CSIRT oder gegebenenfalls der zuständigen Behörde über einen vom CSIRT oder gegebenenfalls der zuständigen Behörde bereitgestellten Kommunikationskanal Folgendes mitteilen: ob die Einrichtung eine Lösegeldforderung erhalten hat und gegebenenfalls von wem, ob ein Lösegeld gezahlt wurde, und wenn ja, in welcher Höhe und an welchen Empfänger oder welche Empfängerseite, gegebenenfalls einschließlich der Anbieter von Kryptowerten und Krypto-Dienstleistungen.“	EU-Mitgliedstaaten Wesentliche und wichtige Einrichtungen	Berichterstattung	Datenfluss

Artikel 1 Absatz 10, Richtlinie Liste von Einrichtungen und Register (Artikel 27 Absatz 1 NIS2)	**Die ENISA erstellt und pflegt ein Register der wesentlichen und wichtigen Einrichtungen sowie der Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, auf der Grundlage der Informationen, die sie von den zentralen Anlaufstellen gemäß Artikel 2 erhalten hat**.	ENISA EU-Mitgliedstaaten (wesentliche und wichtige Einrichtungen nach NIS2, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen)	Die ENISA erstellt und pflegt ein Register.	Digitale Lösung Digitaler öffentlicher Dienst
Artikel 1 Absatz 11, Richtlinie Liste von Einrichtungen und Register (Artikel 27 Absatz 4 NIS2)	**„(4) Nach Erhalt der in Artikel 3 Absatz 4 genannten Angaben leitet die zentrale Anlaufstelle des betreffenden Mitgliedstaats diese unverzüglich an die ENISA weiter.“**	ENISA EU-Mitgliedstaaten	Mitgliedstaaten, die Informationen an die ENISA weitergeben	Datenfluss
Artikel 1 Absatz 12, Richtlinie Amtshilfe (Artikel 37a Absätze 1, 2 und 3 NIS2)	**1. Die ENISA unterstützt die Mitgliedstaaten** bei der Amtshilfe im Sinne des Artikels 37 und **trägt dazu bei, solche Kooperationsprozesse** für wesentliche und wichtige Einrichtungen **zu erleichtern**, ... 2. Die ENISA **führt eine umfassende Analyse durch** … Die **ENISA entwickelt in Zusammenarbeit** mit der Kommission und der Kooperationsgruppe eine Methodik. Der Bericht wird jährlich aktualisiert. 3. Gegebenenfalls gibt die ENISA Empfehlungen ab, entwickelt Leitlinien, unterstützt ...	ENISA EU-Mitgliedstaaten Wesentliche und wichtige Einrichtungen im Sinne der NIS-2-Richtlinie EU-Kommission	Die ENISA unterstützt die Mitgliedstaaten und trägt dazu bei, den Kooperationsprozess zu erleichtern. Analyse, Leitlinien, Methodik, Berichte.	Datenverarbeitung Datenfluss
Artikel 1 Absatz 12, Richtlinie Amtshilfe (Artikel 37a Absatz 4 NIS2)	4. Für die Zwecke des Absatzes 4 Buchstabe e übermitteln die zuständigen Behörden **der betreffenden**	ENISA EU-Mitgliedstaaten	Informationsaustausch	Datenfluss

	Mitgliedstaaten der ENISA, soweit verfügbar, Folgendes ... 5. Erhält ein Mitgliedstaat Amtshilfe gemäß Artikel 37 Absatz 1 Unterabsatz 1 Buchstabe c, **so teilt die zentrale Anlaufstelle der ENISA mit**, dass Amtshilfe geleistet wurde.			
Artikel 119 Ausübung der Befugnisübertragung	3. Sobald die Kommission einen delegierten Rechtsakt erlässt, **übermittelt sie ihn gleichzeitig** dem Europäischen Parlament und dem Rat.	EU-Kommission Europäisches Parlament Rat	Dem EP und dem Rat übermittelte Informationen	Datenfluss
Artikel 120 Bewertung und Überarbeitung	1. Bis zum [TT.MM.JJJJ] und danach alle fünf Jahre bewertet die Kommission im Einklang mit ihren Leitlinien die Leistung der ENISA im Verhältnis zu ihren Zielen, ihrem Mandat, ihrem Auftrag, ihren Aufgaben, ihrer Leitung und ihrem Standort. 5. Die Kommission legt die Ergebnisse der Bewertung dem Europäischen Parlament, dem Rat und dem Verwaltungsrat vor. Die Ergebnisse der Bewertung werden veröffentlicht.	ENISA Kommission Öffentlichkeit	Erhebung und Analyse von Daten, Veröffentlichung von Informationen	Datenverarbeitung Datenfluss

4.2. Daten

Allgemeine Beschreibung der erfassten Daten und aller damit zusammenhängenden Standards/Spezifikationen

Art der Daten	Anforderung(en)	Standard und/oder Spezifikation (falls zutreffend)
Daten im Zusammenhang mit Analysen/Berichten, die für die Cybersicherheitsresilienz und die Gesellschaft von Bedeutung sind	**Artikel 5 Absatz 1 Buchstaben a, b, c, e, f, h** **Artikel 5 Absätze 2, 3 und 4** **Artikel 6** **Artikel 7** **Artikel 8** **Artikel 9** **Artikel 10** **Artikel 11 Absatz 2 Buchstaben b und c** **Artikel 12 Absatz 4** **Artikel 15** **Artikel 1 Absatz 7, Richtlinie**	Bei der Durchführung der in Artikel 11 Absatz 1 Buchstaben a bis e sowie Absatz 2 aufgeführten Tätigkeiten stützt sich die ENISA auf ihre eigenen Analysen und gegebenenfalls auf die Informationen, die sie bei der Wahrnehmung ihrer Aufgaben erhält, einschließlich a) Informationen aus öffentlich zugänglichen Quellen, einschließlich öffentlich bekannter Schwachstellen in IKT-Produkten oder -Diensten, die in der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank enthalten sind; b) Informationen, die von den Mitgliedstaaten, den Einrichtungen der Union, dem CERT-EU, Partnern aus dem Privatsektor oder nichtstaatlichen Partnern sowie Drittländern und internationalen Organisationen weitergegeben werden, vorbehaltlich etwaiger Beschränkungen der Weiterverbreitung dieser Informationen durch sichtbare Kennzeichnungen. Die ENISA gibt Leitlinien für die Interoperabilität der für die Informationsweitergabe verwendeten Netz- und Informationssysteme heraus, auch in Bezug auf grenzübergreifende Cyber-Hubs gemäß Artikel 6 Absatz 3 der Verordnung (EU) 2025/38.
Daten, die für die operative Zusammenarbeit und die Lageerfassung von Bedeutung sind	**Artikel 10 Absatz 4 Buchstaben a bis g** **Artikel 10 Absatz 6** **Artikel 11 Absatz 1 Buchstaben a bis g** **Artikel 11 Absatz 2 Buchstaben a, b, c**	**Standards für die Vertraulichkeit und die Behandlung sensibler Informationen** Bei der Durchführung der in Artikel 11 Absatz 1 Buchstaben a bis e sowie Absatz 2 aufgeführten Tätigkeiten stützt sich die ENISA auf ihre eigenen Analysen und gegebenenfalls auf die Informationen, die sie bei der Wahrnehmung ihrer Aufgaben

	Artikel 11 Absatz 3 **Artikel 11 Absatz 4** **Artikel 13 Absatz 2** **Artikel 15** **Artikel 16 Absatz 2 Buchstabe e**	erhält, einschließlich a) Informationen aus öffentlich zugänglichen Quellen, einschließlich öffentlich bekannter Schwachstellen in IKT-Produkten oder -Diensten, die in der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank enthalten sind; b) Informationen, die von den Mitgliedstaaten, den Einrichtungen der Union, dem CERT-EU, Partnern aus dem Privatsektor oder nichtstaatlichen Partnern sowie Drittländern und internationalen Organisationen weitergegeben werden, vorbehaltlich etwaiger Beschränkungen der Weiterverbreitung dieser Informationen durch sichtbare Kennzeichnungen.
Daten, die für die Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen und die Erteilung von Befugnissen an Anbieter von Bedeutung sind **Daten, die für die Ziele, den Zweck und den Inhalt europäischer Systeme für die Cybersicherheitszertifizierung von Bedeutung sind**	**Artikel 17** **Artikel 18** **Artikel 19-23** **Artikel 72, 73, 74, 75, 76, 77, 79, 81, 83, 84**	Ein System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen umfasst ... Vorschriften über die Aufbewahrung von Aufzeichnungen durch befugte Bescheinigungsanbieter Befugte Anbieter stellen sicher, dass elektronische Einzelbescheinigungen der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen auf Ersuchen einer Einzelperson als elektronische Attributsbescheinigungen in einem Format ausgestellt werden, das in den europäischen Brieftaschen für die digitale Identität gemäß der Verordnung (EU) Nr. 910/2014 gespeichert werden kann. Die Kommission und die ENISA sollten sich bei der Einrichtung eines europäischen Systems für die Cybersicherheitszertifizierung in Bezug auf Daten an die einschlägigen Bestimmungen des Unionsrechts halten.

Daten in Verbindung mit der Gestaltung des europäischen Rahmens für die Cybersicherheitszertifizierung	**Artikel 85, 86, 88, 89, 90, 92, 93, 94, 95, 96, 97**	Die ENISA, die Konformitätsbewertungsstellen und die nationalen Behörden für die Cybersicherheitszertifizierung sollten die Vertraulichkeit der Daten gewährleisten und die Bestimmungen eines einschlägigen Systems befolgen, in dem auf internationale Normen verwiesen wird, in denen die Anforderungen festgelegt sind.
Daten, die für die internen Funktionen der ENISA (Haushalt, einheitliches Programmplanungsdokument, interne Strategien) von Bedeutung sind	**Artikel 25** **Artikel 28 Absatz 1** **Artikel 30** **Artikel 31 Absatz 8** **Artikel 32 Absätze 3 und 5** **Artikel 35 Absätze 5 und 6** **Artikel 36-43** **Artikel 44** **Artikel 45** **Artikel 47 Absatz 10** **Artikel 48-49** **Artikel 52, Artikel 58**	**Muster und Leitlinien für die Finanzregelung; interne Leitlinien**
Personenbezogene Daten	**Artikel 22** **Titel II Kapitel III Abschnitt 6 – Beschwerdekammer** **Artikel 66** **Artikel 80 Absatz 1 Buchstaben c und x** **Artikel 81 Absatz 2** **Artikel 88 Absatz 6 Buchstabe h**	**Verordnung (EU) 2018/1725** **Verordnung (EU) 2016/679**

	Artikel 95 **Artikel 96**	
Daten, die im Rahmen der Durchführung koordinierter Risikobewertungen, der Entwicklung von Risikoszenarien und der Ermittlung wichtiger IKT-Assets erhoben und analysiert werden	**Artikel 98** **Artikel 99** **Artikel 102** **Artikel 103** **Artikel 105**	Unbeschadet des Artikels 13 der Verordnung (EU) 2024/2847 und des Artikel 21 der Verordnung (EU) 2022/2555
Daten in Bezug auf Drittländer / Einrichtungen aus Drittländern	**Artikel 100 Absätze 1, 3 und 4** **Artikel 104** **Artikel 105** **Artikel 107** **Artikel 113**	Nicht zutreffend
Daten in Bezug auf nationale Behörden	**Artikel 112** **Artikel 114** **Artikel 116**	Nicht zutreffend
Daten, die für Risikobewertungen von Bedeutung sind	**Artikel 5 Absatz 2**	**Standards für die Vertraulichkeit und die Behandlung sensibler Informationen**
Amtshilfe zwischen den Mitgliedstaaten	**Artikel 5 Absatz 1 Buchstabe g der Verordnung und Artikel 1 Nummer 12 der Richtlinie**	**/**

Vereinbarkeit mit der europäischen Datenstrategie

Erläutern Sie, inwiefern die Anforderung(en) mit der europäischen Datenstrategie vereinbar ist/sind.

Die Anforderungen im CSA2-Vorschlag sind an die europäische Datenstrategie angepasst und haben keine spezifischen Auswirkungen.

Vereinbarkeit mit dem Grundsatz der einmaligen Erfassung

Erläutern Sie, inwiefern der Grundsatz der einmaligen Erfassung berücksichtigt wurde und inwiefern die Möglichkeit der Weiterverwendung vorhandener Daten geprüft wurde.

Eines der Ziele des Vorschlags besteht darin, die Vereinfachungsbemühungen der Kommission zu maximieren und den Verwaltungsaufwand für die Mitgliedstaaten und die Interessenträger zu verringern. In den letzten Jahren ist die ENISA zu einer Informationsdrehscheibe für Informationen aus verschiedenen Quellen geworden. In diesem Sinne sind zahlreiche der Aufgaben der ENISA mit der Weiterverwendung und dem Recycling von Informationen für die Zwecke verschiedener Analysen verbunden. Zum Beispiel: die Weiterverwendung von gemäß den Artikeln 23 und 30 der Richtlinie (EU) 2022/2555 gemeldeten Informationen für bestimmte Zwecke; Informationen, die gemäß Artikel 14 Absätze 1 bis 3, Artikel 15 und Artikel 17 Absätze 1 und 3 der Verordnung (EU) 2024/2847 gemeldet, weitergegeben oder analysiert werden. Bei den Bestimmungen des Rahmens für die Lieferkette wird davon ausgegangen, dass seine Umsetzung durch die gemäß Artikel 22 der Richtlinie (EU) 2022/2555 erhaltenen Daten unterstützt wird, was die Weiterverwendung von Informationen und die Koordinierung zeigt.

Erläutern Sie, wie neu geschaffene Daten auffindbar, zugänglich, interoperabel und wiederverwendbar sind und hohen Standards entsprechen.

Im Legislativvorschlag ist ausdrücklich festgelegt, wann Daten öffentlich zugänglich gemacht werden sollten. Der Vorschlag berücksichtigt die Art der Bestimmungen unter strikter Berücksichtigung von Sicherheits- und Vertraulichkeitsaspekten, weshalb nicht alle Daten, die im Rahmen der Überprüfung des CSA generiert werden, für den öffentlichen Verbrauch bestimmt sind. Für die erforderlichen Bestimmungen wurde die Angleichung an die europäische Brieftasche für die digitale Identität sichergestellt. Die ENISA hat die Aufgabe, Frühwarndienste in einem maschinenlesbaren Format anzubieten.

Datenflüsse

Allgemeine Beschreibung der erfassten Daten und aller damit zusammenhängenden Standards/Spezifikationen

Art der Daten	Erläuterung des Datenflusses	Verweise
Die ENISA stellt Berichte und Analysen, technische Leitlinien und bewährte Verfahren bereit.	Hierbei handelt es sich um einen Datenfluss, der an die Interessenträger der ENISA gerichtet ist und die Umsetzung der EU-Politik und des EU-Rechts unterstützt. In diesen Datenflüssen sammelt die ENISA Informationen, meist aus öffentlichen Quellen, erstellt Analysen und teilt die Ergebnisse mit ihren Interessenträgern. Die ENISA führt bestimmte Aufgaben – auch auf Ersuchen der Kommission – aus.	Artikel 5 Absatz 1 Buchstaben a, b, c, e, f und h Artikel 5 Absatz 2, Artikel 5 Absatz 3, Artikel 5 Absatz 5 Artikel 6 Artikel 7 Artikel 8 Artikel 9 Artikel 10 Artikel 11 Absatz 2 Artikel 11 Absatz 4 Artikel 14
Datenflüsse zwischen der Kommission, der ENISA, den Mitgliedstaaten und anderen einschlägigen Akteuren innerhalb des Cybersicherheitsökosystems der EU im Zuge der operativen Zusammenarbeit.	Diese Art von Datenflüssen wird für die Zwecke der operativen Zusammenarbeit und des Lagebewusstseins eingerichtet. Der Informationsaustausch erfolgt in beide Richtungen. Es werden operative Daten ausgetauscht.	Artikel 10 Absatz 4 Buchstaben a bis g Artikel 11 Absatz 1 Buchstaben b bis g Artikel 11 Absatz 2 Buchstaben a und b Artikel 11 Absatz 3 Artikel 15 Artikel 16 Absatz 2 Buchstabe e
Datenflüsse zur Unterstützung des ECSF und der Systeme europäischer Einzelbescheinigungen von	Diese Datenflüsse unterstützen den gegenseitigen Austausch in Bezug auf – die Pflege und Verbreitung des ECSF mit einem Austausch zwischen der ENISA und den	Artikel 19 bis 23 Artikel 36 bis 43

Cybersicherheitskompetenzen und deren Umsetzung	Mitgliedern ihrer Ad-hoc-Arbeitsgruppe sowie zwischen der ENISA und der Kommission; – die Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen mit einem Austausch zwischen der ENISA und den Mitgliedern ihrer Ad-hoc-Arbeitsgruppe sowie zwischen der ENISA, der Kommission und den Mitgliedstaaten; – die Umsetzung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen mit einem Austausch zwischen Antragstellern und der ENISA; – Datenflüssen zwischen der Beschwerdekammer, der ENISA, der Kommission und den Antragstellern.	
Daten, die für die Ziele, den Zweck und den Inhalt europäischer Systeme für die Cybersicherheitszertifizierung von Bedeutung sind	Diese Art von Datenflüssen ist für die Planung, Inauftraggabe, Entwicklung, Annahme und Pflege (einschließlich einer möglichen Überprüfung) europäischer Systeme für die Cybersicherheitszertifizierung relevant. Dies betrifft insbesondere die Einbeziehung und fachliche Beratung der Interessenträger, der ENISA und der Behörden der Mitgliedstaaten durch die ECCG in verschiedenen Phasen des Verfahrens. Darüber hinaus stehen zusätzliche Datenflüsse im Zusammenhang mit der Bereitstellung einschlägiger Informationen für die breite Öffentlichkeit über eigene Websites der Kommission und der ENISA. Schließlich sieht der Rahmen die öffentliche Verfügbarkeit zusätzlicher Cybersicherheitsinformationen von Herstellern oder Anbietern von IKT-Produkten, -Diensten oder -Prozessen vor, für selbst eine EU-Konformitätserklärung oder ein europäisches Cybersicherheitszertifikat ausgestellt wurde.	Artikel 18 Artikel 19 Artikel 72, 73, 74, 75, 76, 77, 79, 81, 83, 84

Daten in Verbindung mit der Gestaltung des europäischen Rahmens für die Cybersicherheitszertifizierung	Diese Datenflüsse unterstützen den gegenseitigen Austausch in Bezug auf – Koordinierung und Verwaltung europäischer Systeme für die Cybersicherheitszertifizierung; – Akkreditierung und Zulassung von Konformitätsbewertungsstellen sowie deren anschließende Notifizierung über die einschlägige Plattform und damit zusammenhängende Verfahren; – Rechtsbehelfsverfahren wie das Recht auf Einlegung einer Beschwerde, auf gerichtlichen Rechtsbehelf oder auf Beschwerde- und Änderungsverfahren.	Artikel 85, 86, 88, 89, 90, 92, 93, 94, 95, 96
Datenflüsse in Bezug auf die Verwaltungstätigkeiten der Agentur	Datenflüsse zwischen der ENISA, dem Verwaltungsrat, den Mitgliedstaaten und der Kommission. Die Informationen beziehen sich auf die Verwaltungstätigkeiten der Agentur, beide Richtungen. In einigen Fällen werden auch Informationen an das Europäische Parlament übermittelt (der entsprechende Datenfluss ist nachstehend dargestellt).	Artikel 25 Artikel 28 Absatz 1 Artikel 30 Artikel 31 Absatz 8 Artikel 32 Absätze 3 und 5 Artikel 35 Absätze 5 und 6 Artikel 36-43 Artikel 44 Artikel 45
An das Europäische Parlament übermittelte Daten	Flüsse an das Europäischen Parlament in Bezug auf die Tätigkeiten und die Wahrnehmung von Aufgaben der ENISA, Haushaltsführung und Finanzmanagement, Zusammenarbeit mit Drittländern und internationalen Organisationen, Anhörung des Kandidaten für das Amt des Exekutivdirektors, Fragen im Zusammenhang mit der europäischen Cybersicherheitszertifizierung.	Artikel 28 Absatz 1 Buchstabe f, Artikel 31 Absatz 8, Artikel 32 Absatz 3, Artikel 44 Absatz 3, Artikel 49 Absatz 6, Artikel 49 Absatz 9, Artikel 70 Absatz 5, Artikel 72 Absätze 4 und 5, Artikel 119 Absatz 3 – Ausübung der Befugnisübertragung, Artikel 120 – Bewertung und Überarbeitung

An den Rat übermittelte Daten	Flüsse an das Europäischen Parlament in Bezug auf die Tätigkeiten und die Wahrnehmung von Aufgaben der ENISA, Haushaltsführung und Finanzmanagement, Zusammenarbeit mit Drittländern und internationalen Organisationen, Anhörung des Kandidaten für das Amt des Exekutivdirektors, mögliche Systeme, die gemäß dem europäischen Rahmen für die Cybersicherheitszertifizierung entwickelt werden.	Artikel 28 Absatz 1 Buchstabe f, Artikel 31 Absatz 8, Artikel 32 Absatz 3, Artikel 32 Absatz 7 Artikel 49 Absatz 6, Artikel 49 Absatz 9, Artikel 70 Absatz 5, Artikel 72 Absätze 4 und 5, Artikel 119 Absatz 3 – Ausübung der Befugnisübertragung, Artikel 120 – Bewertung und Überarbeitung
Datenflüsse in Bezug auf die Einreichung einer Beschwerde	Bearbeitung von Beschwerden natürlicher oder juristischer Personen im Zusammenhang mit europäischen Cybersicherheitszertifikaten, die von nationalen Behörden für die Cybersicherheitszertifizierung ausgestellt wurden, oder mit europäischen Cybersicherheitszertifikaten, die von Konformitätsbewertungsstellen im Einklang mit Artikel 84 Absatz 4 ausgestellt wurden, oder im Zusammenhang mit EU-Konformitätserklärungen Natürliche und juristische Personen haben das Recht, bei dem Aussteller eines europäischen Cybersicherheitszertifikats oder – wenn sich die Beschwerde gegen ein von einer Konformitätsbewertungsstelle ausgestelltes europäisches Cybersicherheitszertifikat richtet – eine Beschwerde einzulegen.	Artikel 55 Absatz 3, Artikel 88 Absatz 7 Buchstabe f, Artikel 96
Datenflüsse in Bezug auf Ransomware-Angriffe	Meldung bestimmter Informationen im Fall von Ransomware-Angriffen	Artikel 1 Absatz 8, Richtlinie

Art der Daten	Anforderung(en)	Akteure, die die Daten bereitstellen	Akteure, die die Daten empfangen	Auslöser für den Datenaustausch	Häufigkeit (falls zutreffend)
Datenfluss zwischen der Kommission und den Mitgliedstaaten im Zusammenhang mit der Durchführung auf Unionsebene koordinierter Sicherheitsrisikobewertungen.	Artikel 99 Sicherheitsrisikobewertungen	Kommission und Mitgliedstaaten	Mitgliedstaaten (NIS-Kooperationsgruppe)	Artikel 99 Sicherheitsrisikobewertungen	Nicht zutreffend
Datenfluss zwischen der Kommission und dem Rat im Zusammenhang mit der Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen	Artikel 100 Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen	Kommission	Rat	Artikel 100 Verifizierung der von einem Drittland ausgehenden Bedrohung durch die Kommission	
Datenflüsse zwischen der Kommission und den Mitgliedstaaten in Bezug auf Risikominderungsmaßnahmen im Falle außergewöhnlicher Umstände	Artikel 103 Absatz 6 Risikominderungsmaßnahmen in der IKT-Lieferketten	Kommission	Mitgliedstaaten	Außergewöhnliche Umstände	Nicht zutreffend

Art der Daten	**Anforderung(en)**	**Akteure, die die Daten bereitstellen**	**Akteure, die die Daten empfangen**	**Auslöser für den Datenaustausch**	**Häufigkeit (falls zutreffend)**
Datenflüsse zwischen der Kommission und den Anbietern sowie der Kommission und den zuständigen Behörden in Bezug auf die Bewertung der Niederlassung, des Eigentums und der Kontrolle der Anbieter	Artikel 104 Absätze 4, 5 und 6 Ermittlung von Hochrisikoanbietern	Anbieter Kommission Zuständige Behörden	Zuständige Behörden Anbieter Kommission	Im Einklang mit Artikel 103 Absatz 1 und in Bezug auf die Verbote gemäß Artikel 111 Absatz 1 erlassene Durchführungsrechtsakte	Nicht zutreffend
Datenfluss zwischen der Kommission und den Mitgliedstaaten in Bezug auf Aufsichtsbefugnisse im Zusammenhang mit der Umsetzung des Rahmens für die Sicherheit der vertrauenswürdigen IKT-Lieferketten	Artikel 112 Absätze 1 und 4 Zuständige Behörden Artikel 114 Aufsichts- und Durchsetzungsmaßnahmen	Mitgliedstaaten	Kommission	Artikel 112 Absätze 1 und 4 Zuständige Behörden Artikel 114 Aufsichts- und Durchsetzungsmaßnahmen (Die Kommission erstellt in Zusammenarbeit mit den Mitgliedstaaten eine Liste der mit Hochrisikoanbietern verbundenen Einrichtungen.)	Nicht zutreffend

Art der Daten	Anforderung(en)	Akteure, die die Daten bereitstellen	Akteure, die die Daten empfangen	Auslöser für den Datenaustausch	Häufigkeit (falls zutreffend)
Datenfluss zwischen der Kommission und Dritten in Bezug auf Ausnahmen	Artikel 105 Ausnahmen für Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von in einem solchen Drittland aus kontrolliert werden	Dritte (Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen (im Sinne des Artikels 100), niedergelassen sind oder von Einrichtungen aus einem solchen Drittland kontrolliert werden) (bei Einreichung eines Antrags auf eine Ausnahme) EU-Kommission (beim Erlass von Beschlüssen)	Kommission (bei Eingang des Antrags auf eine Ausnahme) Dritte (Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen (im Sinne des Artikels 100), niedergelassen sind oder von Einrichtungen aus einem solchen Drittland kontrolliert werden) (nach Eingang des Beschlusses der Kommission)	Beschluss nach Artikel 100 – Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen	Nicht zutreffend
Datenfluss zwischen den Mitgliedstaaten und Dritten in Bezug auf Verbote für elektronische Kommunikationsnetze	Artikel 111 Verbote für mobile, feste und satellitengestützte elektronische Kommunikationsnetze	Mitgliedstaaten (zuständige Behörden)	Dritte (Anbieter mobiler, fester und satellitengestützter elektronischer Kommunikationsnetze)	Die gemäß dieser Verordnung benannte zuständige Behörde unterrichtet die gemäß der Verordnung (EU) XX/XXXX [DNA-Vorschlag] zuständige	Nicht zutreffend

Art der Daten	Anforderung(en)	Akteure, die die Daten bereitstellen	Akteure, die die Daten empfangen	Auslöser für den Datenaustausch	Häufigkeit (falls zutreffend)
				Behörde unverzüglich über die Maßnahmen, die Anbietern von mobilen, festen und satellitengestützten elektronischen Kommunikationsnetzen auferlegt wurden.	
Datenfluss zwischen der Kommission und den Mitgliedstaaten im Zusammenhang mit dem Netz für die Zusammenarbeit und den Unterstützungsdiensten	Artikel 113 Netz für die Zusammenarbeit und Unterstützungsdienste der Kommission	Kommission Mitgliedstaaten (zuständige Behörden)	Kommission Mitgliedstaaten (zuständige Behörden)	Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen	
Datenfluss zwischen den Mitgliedstaaten und Dritten in Bezug auf Aufsichts- und Durchsetzungsmaßnahmen	Artikel 114 Aufsichts- und Durchsetzungsmaßnahmen	Dritte (Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 aufgeführten Art)	Mitgliedstaaten (zuständige Behörden)	Umsetzung der in Titel IV vorgesehenen Maßnahmen	
Datenfluss zwischen den Mitgliedstaaten in Bezug auf Amtshilfe	Artikel 116 Amtshilfe	Mitgliedstaaten	Mitgliedstaaten	Wenn eine in Anhang I oder II der Richtlinie (EU) 2022/2555 genannte Einrichtung ihre Dienste	Nicht zutreffend

Art der Daten	Anforderung(en)	Akteure, die die Daten bereitstellen	Akteure, die die Daten empfangen	Auslöser für den Datenaustausch	Häufigkeit (falls zutreffend)
				in mehr als einem Mitgliedstaat erbringt oder wenn sie ihre Dienste in einem oder mehreren Mitgliedstaaten erbringt und sich ihre wichtigen IKT-Assets in einem oder mehreren anderen Mitgliedstaaten befinden, so arbeiten die zuständigen Behörden der betreffenden Mitgliedstaaten zusammen und unterstützen einander.	

4.3. Digitale Lösungen

Allgemeine Beschreibung der digitalen Lösungen

Für jede digitale Lösung Erläuterung, inwiefern diese mit geltenden digitalen Strategien und Rechtsvorschriften im Einklang steht.

Digitale Lösung	Anforderung(en)	Wichtigste vorgeschriebene Funktionen	Zuständige Stelle	Inwiefern wird Zugänglichkeit gewährleistet	Wie wird die Wiederverwendbarkeit berücksichtigt?	Einsatz von KI-Technologien (falls zutreffend)

				?		
Die ENISA, die die **Sekretariatsgeschäfte des CSIRTs-Netzwerks und des EU-CyCLONe** wahrnimmt, verwendet innerhalb des CSIRTs-Netzwerks und des EU-CyCLONe **sichere Kommunikationsinstrumente**, die von Rechtsträgern bereitgestellt werden, die nicht in Drittländern niedergelassen sind bzw. von Drittländern oder von Staatsangehörigen von Drittländern kontrolliert werden.	Artikel 10 Absätze 2, 3 und 5	Keine öffentlichen Informationen	ENISA	Keine öffentlichen Informationen	Keine öffentlichen Informationen	Keine öffentlichen Informationen
in Zusammenarbeit mit dem EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission, Europol, dem CERT-EU und anderen einschlägigen Einrichtungen der Union **Entwicklung von Ablagen verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen**, einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren.	Artikel 11 Absatz 1 Buchstabe a	verifizierte, zuverlässige Erkenntnisse über Cyberbedrohungen, einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren	ENISA EU-CyCLONe, CSIRTs-Netzwerk, Kommission, Europol, CERT-EU und einschlägige Einrichtungen der Union	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Die ENISA **unterhält eine Ablage der gewonnenen Erkenntnisse**.	Artikel 14 Absatz 2	Die ENISA unterhält eine Ablage der aus Übungen gewonnenen Erkenntnisse und gibt den	ENISA	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

		Mitgliedstaaten und gegebenenfalls den Einrichtungen der Union Empfehlungen dazu, wie die gewonnenen Erkenntnisse wirksam und effizient genutzt werden können.				
Die ENISA sorgt für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung operativer technischer Instrumente einschließlich **Plattformen** für die Cybersicherheit auf Unionsebene, insbesondere der gemäß Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 eingerichteten einheitlichen Meldeplattform [und der gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstelle zur Meldung von Vorfällen,] oder von Testinstrumenten zur Unterstützung der Durchführung von Konformitätsbewertungsverfahren im Einklang mit den einschlägigen Rechtsvorschriften der Union.	Artikel 15	Einheitliche Meldeplattform Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 [Zentrale Anlaufstelle Artikel 23a der Richtlinie (EU) 2022/2555]	ENISA	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Pflege der gemäß Artikel 12		Artikel 12 Absatz 2 der	ENISA	Nicht	Nicht zutreffend	Nicht

Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank und **Bereitstellung von Schwachstellenmanagementdiensten**	Artikel 16 Absatz 2	Richtlinie (EU) 2022/2555 Pflege der Datenbank und Bereitstellung von Schwachstellenmanagementdiensten		zutreffend		zutreffend
Die ENISA unterhält eine eigene Website mit öffentlichen Informationen und aktualisiert diese regelmäßig.	Artikel 19-23	Unterhalt und regelmäßige Aktualisierung einer eigenen Website mit öffentlichen Informationen über den ECSF, einschließlich des Rahmens und des Zeitplans für die Aktualisierung; Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, deren Fortschritte und Zeitpläne für deren Entwicklung; Gebühren in Verbindung mit jedem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen: die voraussichtlichen Kosten einer europäischen Einzelbescheinigung von Cybersicherheitskompetenzen; die Liste befugter Bescheinigungsanbieter.	ENISA	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Die **Kommission unterhält eine eigene öffentliche Website und aktualisiert diese regelmäßig**.	Artikel 72	Folgende Informationen: a) europäische Systeme für die Cybersicherheitszertifizierung, deren Entwicklung in Auftrag gegeben wurde; b) strategische Prioritäten für die Harmonisierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder Sicherheitsanforderungen des Unionsrechts, einschließlich möglicher Bereiche, für die ein europäisches System für die Cybersicherheitszertifizierung in Auftrag gegeben werden könnte.	EU-Kommission	Einhaltung der Leitlinien	Einhaltung der Leitlinien	Nicht zutreffend
Die ENISA unterhält eine eigene Zertifizierungswebsite.	Artikel 79	Bereitstellung von Informationen zu a) europäischen Systemen für die Cybersicherheitszertifizierung; b) den mit der Pflege jedes europäischen Systems für die Cybersicherheitszertifizierung verbundenen Gebühren; c) einschlägigen technischen Spezifikationen der ENISA; d) europäischen Cybersicherheitszertifikaten und	ENISA	Einhaltung der Leitlinien	Einhaltung der Leitlinien	Nicht zutreffend

		EU-Konformitätserklärungen, einschließlich Informationen in Bezug auf solche Zertifikate und Erklärungen, die nicht mehr gültig sind, ausgesetzt oder widerrufen wurden oder abgelaufen sind; e) einschlägigen zusätzlichen Cybersicherheitsinformationen im Einklang mit Artikel 84 Absatz 2; f) Zusammenfassungen gegenseitiger Begutachtungen gemäß Artikel 89 Absatz 7; g) technischen Spezifikationen, auf die in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 Bezug genommen wird.				
Register (von Ausnahmen für Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert werden)	Artikel 107 Register	Die Kommission führt ein öffentlich zugängliches Register ihrer in Artikel 105 Absatz 4 genannten Beschlüsse. Das Register enthält die Namen der Einrichtungen, die Gegenstand solcher Beschlüsse sind. Die Kommission aktualisiert es regelmäßig.	Kommission	„Die Kommission führt ein öffentlich zugängliches Register.“	Nicht zutreffend	Nicht zutreffend

Plattform (für die Zusammenarbeit und den Informationsaustausch zwischen der Kommission und den zuständigen Behörden)	Artikel 113	Die Kommission richtet ein Netz für die Zusammenarbeit der zuständigen Behörden der Mitgliedstaaten und der Kommission ein, das als Plattform für die Zusammenarbeit und den Informationsaustausch dient. Die Kommission stellt dem Netz administrative Unterstützung bereit.	Kommission	Nicht öffentlich, nur für zuständige Behörden	Nicht zutreffend	Nicht zutreffend
Die ENISA richtet ein Register wesentlicher und wichtiger Einrichtungen sowie von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, **ein** und pflegt dieses.	Artikel 1 Absatz 11, Richtlinie	Register wesentlicher und wichtiger Einrichtungen sowie von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen	ENISA	Nicht zutreffend	Auf der Grundlage der gemäß Artikel 2 von den zentralen Anlaufstellen erhaltenen Informationen (Artikel 27 der NIS-2-Richtlinie)	Nicht zutreffend

In der vorstehenden Tabelle enthaltene digitale Lösungen

Digitale und/oder sektorspezifische Strategie (falls anwendbar)	Erläuterung der Vereinbarkeit
KI-Verordnung	Nicht zutreffend
EU-Rahmen für Cybersicherheit	Nicht zutreffend
eIDAS	Nicht zutreffend
Einheitliches digitales Zugangstor und IMI	Nicht zutreffend
Sonstige	Nicht zutreffend

Allgemeine Beschreibung der von den Anforderungen betroffenen digitalen öffentlichen Dienste

Digitaler öffentlicher Dienst oder Kategorie digitaler öffentlicher Dienste	Beschreibung	Anforderung(en)	Lösung(en) für ein interoperables Europa (NICHT ZUTREFFEND)	Andere Interoperabilitätslösung(en)
ENISA als Sekretariat der Netzwerke und Einsatz sicherer Kommunikationsinstrumente	Die ENISA nimmt gemäß Artikel 15 Absatz 2 der Richtlinie (EU) 2022/2555 die Sekretariatsgeschäfte des CSIRTs-Netzwerks wahr. Die ENISA nimmt gemäß Artikel 16 Absatz 2 der Richtlinie (EU) 2022/2555 die Sekretariatsgeschäfte des EU-CyCLONe wahr und stellt [die gemäß Artikel 23a der Richtlinie	Artikel 11	//	Nicht zutreffend

	(EU) 2022/2555 eingerichtete zentrale Anlaufstelle zur Meldung von Vorfällen sowie] Testinstrumente zur Unterstützung der Durchführung von Konformitätsbewertungsverfahren im Einklang mit den einschlägigen Rechtsvorschriften der Union bereit. Die ENISA setzt innerhalb des CSIRTs-Netzwerks und des EU-CyCLONe sichere Kommunikationsinstrumente ein, die von Rechtsträgern bereitgestellt werden, die nicht in Drittländern niedergelassen sind bzw. von Drittländern oder von Staatsangehörigen von Drittländern kontrolliert werden.			
Frühwarnungen	Ausgabe von Frühwarnungen	Artikel 11 Artikel 12		
Unterstützung in Bezug auf einen bestimmten potenziellen oder andauernden Sicherheitsvorfall bzw. eine entsprechende Cyberbedrohung	Auf Ersuchen eines oder mehrerer Mitgliedstaaten Bereitstellung von Beratung und Bewertungen in Bezug auf einen bestimmten potenziellen oder andauernden Sicherheitsvorfall bzw. eine entsprechende Cyberbedrohung, auch durch die Bereitstellung von Sachkenntnis und die Erleichterung der technischen Bewältigung solcher Vorfälle sowie durch die Unterstützung der freiwilligen Weitergabe einschlägiger Informationen und technischer Lösungen zwischen den Mitgliedstaaten;	Artikel 10		
Unterstützung des koordinierten Managements	Beitrag zur Unterstützung des koordinierten Managements von	Artikel 10		

von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene	Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene, insbesondere durch Unterstützung des EU-CyCLONe bei der Erstellung von Berichten an die politische Ebene und durch Erleichterung der zeitnahen Informationsweitergabe zwischen dem CSIRTs-Netzwerk und dem EU-CyCLONe.			
Ablagen verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen	In Zusammenarbeit mit dem EU-CyCLONe, dem CSIRTs-Netzwerk, der Kommission, Europol, dem CERT-EU und anderen einschlägigen Einrichtungen der Union Entwicklung von Ablagen verifizierter, zuverlässiger Erkenntnisse über Cyberbedrohungen, einschließlich Trends bei Sicherheitsvorfällen, Taktiken, Techniken und Verfahren.	Artikel 11		
Ablage gewonnener Erkenntnisse	Die ENISA unterhält eine Ablage der aus diesen Übungen gewonnenen Erkenntnisse und gibt den Mitgliedstaaten und gegebenenfalls den Einrichtungen der Union Empfehlungen dazu, wie die gewonnenen Erkenntnisse wirksam und effizient genutzt werden können.	Artikel 14		
Die ENISA sorgt für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung operativer technischer Instrumente einschließlich Plattformen.	Die ENISA sorgt für die Einrichtung, die Bereitstellung, den Betrieb, die Pflege und erforderlichenfalls die Aktualisierung operativer technischer Instrumente einschließlich Plattformen für die Cybersicherheit auf Unionsebene, insbesondere der gemäß Artikel 16 Absatz 1 der Verordnung (EU) 2024/2847 eingerichteten	Artikel 15		

	einheitlichen Meldeplattform [und der gemäß Artikel 23a der Richtlinie (EU) 2022/2555 eingerichteten zentralen Anlaufstelle zur Meldung von Vorfällen] sowie von Testinstrumenten zur Unterstützung der Durchführung von Konformitätsbewertungsverfahren im Einklang mit den einschlägigen Rechtsvorschriften der Union.			
Pflege der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank	Pflege der gemäß Artikel 12 Absatz 2 der Richtlinie (EU) 2022/2555 eingerichteten europäischen Schwachstellendatenbank Bereitstellung von Schwachstellenmanagementdiensten für Interessenträger, aufbauend auf der europäischen Schwachstellendatenbank und unter Rückgriff auf die der ENISA zur Verfügung stehenden einschlägigen Informationen. Aufnahme einer strukturierten Zusammenarbeit mit Organisationen, die ähnliche Programme, Register oder Datenbanken wie die europäische Schwachstellendatenbank bereitstellen. Aktive Unterstützung der gemäß Artikel 12 Absatz 1 der Richtlinie 2022/2555 als Koordinatoren benannten CSIRTs im Hinblick auf die Steuerung der koordinierten Offenlegung von Schwachstellen, die erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten nach sich ziehen könnten.	Artikel 16		

	Entwicklung und Aufrechterhaltung von Methoden und Governance-Mechanismen für die Ermittlung und koordinierte Offenlegung von Schwachstellen in Zusammenarbeit mit den zuständigen nationalen Behörden, den CSIRTs, der Branche und der Forschungsgemeinschaft.			
Ausarbeitung möglicher europäischer Systeme für die Cybersicherheitszertifizierung („mögliche Systeme“)	Ausarbeitung möglicher europäischer Systeme für die Cybersicherheitszertifizierung („mögliche Systeme“) für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und die Cyberabwehr von Einrichtungen und damit verbundener technischer Spezifikationen gemäß Artikel 74. Pflege der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 75, auch im Hinblick auf eine mögliche Überprüfung der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 76.	Artikel 17		
Die ENISA ist für die Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen zuständig.	Die ENISA ist für die Entwicklung und Pflege von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen zuständig. Die ENISA trifft eine begründete Entscheidung, mit der sie entweder dem Antragsteller die Befugnis zur Ausstellung europäischer Einzelbescheinigungen für die Bereitstellung und Pflege der Systeme	Artikel 20-22		

	und der Befugnis erteilt, die Befugnis nicht erteilt oder die Bearbeitung des Antrags aufgrund unzureichender vom Antragsteller vorgelegter Informationen oder aufgrund der Untätigkeit des Antragstellers infolge eines Ersuchens der ENISA um zusätzliche Informationen abschließt.			
Die ENISA unterhält eine eigene Website und aktualisiert diese regelmäßig.	Die ENISA unterhält eine eigene Website mit öffentlichen Informationen zu Folgendem und aktualisiert diese regelmäßig: a) ECSF, einschließlich des Rahmens und des Zeitplans für die Aktualisierung; b) Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, deren Fortschritte und Zeitpläne für deren Entwicklung; c) die Gebühren im Zusammenhang mit jedem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen, das gemäß Artikel 47 dieser Verordnung angenommen wird; d) die voraussichtlichen Kosten einer europäischen Einzelbescheinigung von Cybersicherheitskompetenzen gemäß Artikel 20 Absatz 4; e) die Liste befugter Bescheinigungsanbieter.	Artikel 23		
Die Kommission unterhält eine eigene öffentliche	Die Kommission unterhält eine eigene Website mit Informationen zu den	Artikel 72		

Website und aktualisiert diese regelmäßig.	folgenden Aspekten und aktualisiert diese regelmäßig: a) europäische Systeme für die Cybersicherheitszertifizierung, deren Entwicklung in Auftrag gegeben wurde; b) strategische Prioritäten für die Harmonisierung von IKT-Produkten, -Diensten und -Prozessen, verwalteten Sicherheitsdiensten oder Sicherheitsanforderungen des Unionsrechts, einschließlich möglicher Bereiche, für die ein europäisches System für die Cybersicherheitszertifizierung in Auftrag gegeben werden könnte.			
Die ENISA unterhält eine eigene Zertifizierungswebsite.	Die ENISA unterhält eine eigene Website mit öffentlichen Informationen zu Folgendem und aktualisiert diese regelmäßig: a) europäischen Systemen für die Cybersicherheitszertifizierung; b) den mit der Pflege jedes europäischen Systems für die Cybersicherheitszertifizierung verbundenen Gebühren; c) einschlägigen technischen Spezifikationen der ENISA; d) europäischen Cybersicherheitszertifikaten und EU-Konformitätserklärungen, einschließlich Informationen in Bezug auf solche Zertifikate und Erklärungen, die nicht mehr gültig sind, ausgesetzt oder widerrufen wurden oder abgelaufen sind; e) einschlägigen zusätzlichen Cybersicherheitsinformationen im	Artikel 79		

	Einklang mit Artikel 84 Absatz 2; f) Zusammenfassungen gegenseitiger Begutachtungen gemäß Artikel 89 Absatz 7; g) technischen Spezifikationen, auf die in einem europäischen System für die Cybersicherheitszertifizierung gemäß Artikel 74 Absatz 10 Bezug genommen wird.			
Untersuchungen	Die Kommission untersucht alle Fälle, in denen sie die Kompetenz einer Konformitätsbewertungsstelle in Bezug auf die Erfüllung oder die dauerhafte Erfüllung der für die Stelle geltenden Anforderungen und die Wahrnehmung der entsprechenden Zuständigkeiten durch eine Konformitätsbewertungsstelle anzweifelt oder ihr Zweifel daran zur Kenntnis gebracht werden. Die Kommission stellt sicher, dass alle im Verlauf ihrer Untersuchungen erlangten sensiblen Informationen vertraulich behandelt werden.	Artikel 94		
Die ENISA richtet ein Register wesentlicher und wichtiger Einrichtungen sowie von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, ein und pflegt dieses.	Register wesentlicher und wichtiger Einrichtungen sowie von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen Auf Anfrage gewährt die ENISA den zuständigen Behörden Zugang zu Informationen über DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von	Artikel 1 Absatz 11, Richtlinie		

	verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, die in diesem Register gespeichert sind, wobei sie gegebenenfalls für den Schutz der Vertraulichkeit der Informationen sorgt.			

4.4. Interoperabilitätsbewertung

Auswirkungen der Anforderung(en) auf die grenzübergreifende Interoperabilität nach digitalem öffentlichen Dienst

Ablagen / Plattformen / Frühwarnungen / Sekretariatsgeschäfte / CVD-Datenbank

Bewertung	Maßnahmen	Mögliche verbleibende Hindernisse
Bewertung der Angleichung an bestehende digitale und sektorspezifische Strategien Bitte führen Sie die ermittelten anwendbaren digitalen und sektorspezifischen Strategien auf.	*Cybersicherheit*	*Keine bekannten Hindernisse*
Bewertung der organisatorischen Maßnahmen für eine reibungslose grenzübergreifende Erbringung digitaler öffentlicher Dienste Bitte führen Sie die geplanten Governance-Maßnahmen auf.	*Verwaltungsrat der ENISA* *CSIRTs-Netzwerk* *EU-CyCLONe* *NIS-Kooperationsgruppe* *All dies sind Foren, in denen Fragen aufgeworfen werden können.*	*Nicht zutreffend*
Bewertung der Maßnahmen, die ergriffen wurden, um ein gemeinsames Verständnis der Daten	*Nicht zutreffend*	*Nicht zutreffend*

zu gewährleisten **Bitte führen Sie solche Maßnahmen auf.**		
Bewertung der Verwendung gemeinsam vereinbarter offener technischer Spezifikationen und Standards **Bitte führen Sie solche Maßnahmen auf.**	*Nicht zutreffend*	*Nicht zutreffend*

Systeme europäischer Bescheinigungen individueller Cybersicherheitskompetenzen

Bewertung	Maßnahmen	Mögliche verbleibende Hindernisse
Bewertung der Angleichung an bestehende digitale und sektorspezifische Strategien **Bitte führen Sie die ermittelten anwendbaren digitalen und sektorspezifischen Strategien auf.**	*Der Vorschlag baut auf COM(2023) 207 final (Akademie für Cybersicherheitskompetenzen) auf: „Dazu wird die ENISA ein Pilotprojekt entwickeln, in dem die Möglichkeit der Einrichtung eines europäischen Zertifizierungssystems für Cybersicherheitskompetenzen geprüft wird.“* *Sie nutzt die Verordnung (EU) 2024/1183 (europäische Brieftasche für die digitale Identität), indem sie Folgendes festlegt: „Die ENISA und die befugten Bescheinigungsanbieter stellen sicher, dass elektronische Bescheinigungen der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen an die europäischen Brieftaschen für die digitale Identität ausgestellt werden.“* *Cybersicherheit* *DSGVO (Aufbewahrung von Aufzeichnungen durch Anbieter)*	*Keine bekannten Hindernisse*

Bewertung der organisatorischen Maßnahmen für eine reibungslose grenzübergreifende Erbringung digitaler öffentlicher Dienste **Bitte führen Sie die geplanten Governance-Maßnahmen auf.**	*Konsultation der Interessenträger bei der Ausarbeitung eines Systems europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen* *Trennung von Tätigkeiten innerhalb der ENISA zur Gewährleistung ihrer unabhängigen Durchführung* *Beschwerdekammer*	*Die Verwendung und Anerkennung von Systemen europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen bleibt für öffentliche und private Einrichtungen freiwillig.*
Bewertung der Maßnahmen, die ergriffen wurden, um ein gemeinsames Verständnis der Daten zu gewährleisten **Bitte führen Sie solche Maßnahmen auf.**	*Entwicklung von Systemen, die unter anderem Vorschriften über Inhalt und Format der Bescheinigungen enthalten* *Befugte Anbieter stellen sicher, dass elektronische Einzelbescheinigungen der europäischen Einzelbescheinigungen von Cybersicherheitskompetenzen auf Ersuchen einer Einzelperson als elektronische Attributsbescheinigungen in einem Format ausgestellt werden, das in den europäischen Brieftaschen für die digitale Identität gespeichert werden kann. Die ENISA stellt den Prüfern Orientierungshilfen bereit und führt obligatorische Fortbildungen für Prüfer zu den Anforderungen und Bewertungsmethoden durch, die in dem System europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen enthalten sind.* *Bereitstellung von öffentlichen Informationen auf einer Website* *Durchführungsrechtsakte zu Gebühren*	*Obwohl die Systeme so detailliert wie möglich sein sollten, damit ein gemeinsames Verständnis sichergestellt und die Umsetzung erleichtert wird, und obwohl die ENISA Leitlinien für Prüfer bereitstellen und obligatorische Fortbildungen für Prüfer durchführen wird, um eine einheitliche Umsetzung der Systeme zu gewährleisten, könnten unvorhergesehene Situationen entstehen, in denen befugte Bescheinigungsanbieter mit der ENISA, anderen Anbietern oder Prüfern interagieren müssen.*
Bewertung der Verwendung gemeinsam vereinbarter offener	*Systeme europäischer Einzelbescheinigungen von Cybersicherheitskompetenzen werden mit*	*Nicht zutreffend*

technischer Spezifikationen und Standards Bitte führen Sie solche Maßnahmen auf.	*Unterstützung einschlägiger Interessenträger entwickelt.*	

Ausarbeitung möglicher europäischer Systeme für die Cybersicherheitszertifizierung („mögliche Systeme“)/Zuweisung von Zahlen an Konformitätsbewertungsstellen

Bewertung	Maßnahmen	Mögliche verbleibende Hindernisse
Bewertung der Angleichung an bestehende digitale und sektorspezifische Strategien Bitte führen Sie die ermittelten anwendbaren digitalen und sektorspezifischen Strategien auf.	*Mit dem Vorschlag wird eine Angleichung der Governance an den neuen Rechtsrahmen angestrebt, insbesondere in Bezug auf die Verordnung (EG) Nr. 765/2008[26]. Der Vorschlag soll die Einhaltung der einschlägigen sektorspezifischen Rechtsvorschriften im Bereich der Cybersicherheit durch die Entwicklung spezieller europäischer Systeme für die Cybersicherheitszertifizierung erleichtern.*	*Keine bekannten Hindernisse*
Bewertung der organisatorischen Maßnahmen für eine reibungslose grenzübergreifende Erbringung digitaler öffentlicher Dienste Bitte führen Sie die geplanten Governance-Maßnahmen auf.	*Europäische Gruppe für die Cybersicherheitszertifizierung, ENISA, Ad-hoc-Arbeitsgruppen, Europäische Versammlung für die Cybersicherheitszertifizierung, Konsultation der Interessenträger bei der Inauftraggabe, Entwicklung und Annahme europäischer Systeme für die Cybersicherheitszertifizierung, Ausschussverfahren für die geplanten Durchführungsrechtsakte in Verbindung mit europäischen Systemen für die Cybersicherheitszertifizierung.*	*Die Verwendung der europäischen Cybersicherheitszertifizierung ist freiwillig, sofern im EU-Recht nichts anderes festgelegt ist.*

Bewertung der Maßnahmen, die ergriffen wurden, um ein gemeinsames Verständnis der Daten zu gewährleisten **Bitte führen Sie solche Maßnahmen auf.**	*In Abschnitt 4.5 aufgeführte Durchführungsrechtsakte*	*Die Verwendung der europäischen Cybersicherheitszertifizierung ist freiwillig, sofern im EU-Recht nichts anderes festgelegt ist.*
Bewertung der Verwendung gemeinsam vereinbarter offener technischer Spezifikationen und Standards **Bitte führen Sie solche Maßnahmen auf.**	*In Abschnitt 4.5 aufgeführte Durchführungsrechtsakte* *Die für das europäische System für die Cybersicherheitszertifizierung festgelegten Anforderungen stehen in Einklang mit den Anforderungen des Unionsrechts.* *Die europäischen Systeme für die Cybersicherheitszertifizierung stützen sich auf die bei der Bewertung angewandten internationalen, europäischen oder nationalen Normen oder, wenn solche Normen nicht verfügbar oder nicht geeignet sind, auf die von der ENISA ausgearbeiteten technischen Spezifikationen und nehmen auf diese Bezug.*	*Nicht zutreffend*

Öffentlich zugängliche Websites

Bewertung	**Maßnahmen**	**Mögliche verbleibende Hindernisse**
Bewertung der Angleichung an bestehende digitale und sektorspezifische Strategien **Bitte führen Sie die ermittelten anwendbaren digitalen und sektorspezifischen Strategien auf.**	*Rechtsakt der EU zur Barrierefreiheit und Richtlinie über den barrierefreien Zugang zu Websites* *Cybersicherheit*	*Keine bekannten Hindernisse*
Bewertung der organisatorischen Maßnahmen für eine reibungslose grenzübergreifende Erbringung digitaler öffentlicher Dienste	*Nicht zutreffend*	*Nicht zutreffend*

Bitte führen Sie die geplanten Governance-Maßnahmen auf.		
Bewertung der Maßnahmen, die ergriffen wurden, um ein gemeinsames Verständnis der Daten zu gewährleisten **Bitte führen Sie solche Maßnahmen auf.**		*Nicht zutreffend*
Bewertung der Verwendung gemeinsam vereinbarter offener technischer Spezifikationen und Standards **Bitte führen Sie solche Maßnahmen auf.**		*Nicht zutreffend*

4.5. Unterstützungsmaßnahmen für die digitale Umsetzung

Allgemeine Beschreibung der Unterstützungsmaßnahmen für die digitale Umsetzung

Beschreibung der Maßnahme	**Anforderung(en)**	**Rolle der Kommission** (falls zutreffend)	**Zu beteiligende Akteure** (falls zutreffend)	**Voraussichtlicher Zeitplan** (falls zutreffend)
Auf der Grundlage des von der ENISA ausgearbeiteten und von der Kommission angenommenen möglichen Systems ist die Kommission befugt, Durchführungsrechtsakte zu erlassen, in denen für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste oder die Cyberabwehr von Einrichtungen, die die Anforderungen der Artikel 80 und	Artikel 75 Absatz 9	Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen.		Nicht zutreffend

81 erfüllen, ein europäisches System für die Cybersicherheitszertifizierung festgelegt wird. Dieser Durchführungsrechtsakt wird nach dem Prüfverfahren gemäß Artikel 118 Absatz 2 erlassen.				
Der Kommission wird die Befugnis übertragen, gemäß Artikel 119 delegierte Rechtsakte zur Änderung des Absatzes 1 zu erlassen, mit denen Sicherheitsziele hinzugefügt oder geändert werden, damit sie den neuesten technologischen Entwicklungen und neuen damit verbundenen Bedrohungen Rechnung tragen, sowie die Befugnis zum Erlass neuer Rechtsvorschriften der Union, in denen die Vermutung der Konformität mit den einschlägigen Cybersicherheitsanforderungen nach diesen Rechtsvorschriften mithilfe der europäischen Cybersicherheitszertifizierung festgelegt werden.	Artikel 80 Absatz 2	Der Kommission wird die Befugnis übertragen, delegierte Rechtsakte zu erlassen.		Nicht zutreffend
Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung gemeinsamer Grundsätze und Musterbestimmungen für die in den Absätzen 1, 2 und 3 genannten Elemente aller europäischen Systeme für die	Artikel 81 Absatz 5	Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen.	ENISA ECCG	Nicht zutreffend

Cybersicherheitszertifizierung zu erlassen. Soweit angemessen und verfügbar, kann ein europäisches System für die Cybersicherheitszertifizierung Verweise auf diese Grundsätze und Musterbestimmungen enthalten. Die in Unterabsatz 1 genannten Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen. Bei der Entwicklung oder Überarbeitung der gemeinsamen Grundsätze und Musterbestimmungen für die Elemente europäischer Systeme für die Cybersicherheitszertifizierung konsultiert die Kommission die ENISA und berücksichtigt gegebenenfalls die Standpunkte der ECCG, einschlägiger Interessenträger und anderer einschlägiger Stellen.				
Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung der Verfahren für Modelle der vorherigen Zustimmung oder der allgemeinen Übertragung gemäß Absatz 4 zu erlassen. Bei der Vorbereitung dieser Durchführungsrechtsakte konsultiert die Kommission die ECCG. Diese Durchführungsrechtsakte werden	Artikel 85 Absatz 5	Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen.	ECCG	Nicht zutreffend

gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.				
In Drittländern ausgestellte Zertifikate für IKT-Produkte, -Dienste und -Prozesse, verwaltete Sicherheitsdienste und die Cyberabwehr von Einrichtungen können im Wege eines Durchführungsrechtsakts oder durch den Abschluss einer Vereinbarung zwischen der Union und dem betreffenden Drittland oder einer internationalen Organisation als den europäischen Cybersicherheitszertifikaten gleichwertig anerkannt werden, wenn die Anforderungen des betreffenden Systems des Drittlands oder einer internationalen Organisation als den Anforderungen der europäischen Systeme für die Cybersicherheitszertifizierung gleichwertig angesehen werden. Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen. Die Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.	Artikel 87 Absatz 1	Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen.		Nicht zutreffend
Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen, um einen Plan für die	Artikel 89 Absatz 6	Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte		Nicht zutreffend

gegenseitige Begutachtung festzulegen, der sich auf einen Zeitraum von mindestens fünf Jahren erstreckt, und darin die Kriterien für die Zusammensetzung des Begutachtungsteams, die Methode für die gegenseitige Begutachtung und den Zeitplan, die Häufigkeit und die übrigen Aufgaben in Verbindung mit der gegenseitigen Begutachtung vorzugeben. Bei der Vorbereitung dieser Durchführungsrechtsakte konsultiert die Kommission die ECCG und die ENISA. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.		zu erlassen.		
Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zur Festlegung der Verfahren, auch für die grenzüberschreitende Zusammenarbeit, für die Zulassung von Konformitätsbewertungsstellen zu erlassen. Bei der Vorbereitung dieser Durchführungsrechtsakte konsultiert die Kommission die ENISA und die ECCG. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.	Artikel 92 Absatz 8	Der Kommission wird die Befugnis übertragen, Durchführungsrechtsakte zu erlassen.	ENISA ECCG	Nicht zutreffend
Der Kommission wird die Befugnis	Artikel 93 Absatz 3	Der Kommission wird die		Nicht zutreffend

übertragen, Durchführungsrechtsakte zu erlassen, um Einzelheiten, Form und Verfahren für Notifizierungen gemäß Absatz 1 festzulegen, einschließlich des Verfahrens für den Einspruch anderer Mitgliedstaaten während des Notifizierungsverfahrens, der eindeutigen Identifizierung von Konformitätsbewertungsstellen sowie der Einzelheiten in Bezug auf die Einschränkung, die Aussetzung oder den Widerruf einer Notifizierung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren erlassen.		Befugnis übertragen, Durchführungsrechtsakte zu erlassen.		
Die Kommission kann Durchführungsrechtsakte im Einklang mit Artikel 100 erlassen, um ein Drittland, für das Cybersicherheitsbedenken in Bezug auf die IKT-Lieferketten bestehen, zu benennen.	Artikel 100 Absatz 2 Benennung von Drittländern, für die Cybersicherheitsbedenken bestehen	Erlass von Durchführungsrechtsakten		Nicht zutreffend Kein Zeitplan, aber die Durchführungsrechtsakte sollten regelmäßig überprüft werden.
Die Kommission kann Durchführungsrechtsakt erlassen, in denen eine oder mehrere der in Artikel 103 Absatz 2 genannten Risikominderungsmaßnahmen festgelegt sind.	Artikel 103 Absatz 2 Risikominderungsmaßnahmen in der IKT-Lieferketten	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend Kein Zeitplan, aber alle 36 Monate zu überprüfen (gemäß dem in Artikel 118 Absatz 2 genannten Prüfverfahren).

Die Kommission kann im Einklang mit Artikel 102 Durchführungsrechtsakten erlassen, um wichtige IKT-Assets zu ermitteln, die zur Herstellung von Produkten oder zur Erbringung von Dienstleistungen durch die in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten von Einrichtungen eingesetzt werden.	Artikel 102 Absatz 1 Ermittlung wichtiger IKT-Assets	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend
Die Kommission kann Durchführungsrechtsakte erlassen, mit denen untersagt wird, von gemäß Artikel 100 Absatz 2 benannten Hochrisikoanbietern bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, in jedweder Form in gemäß Artikel 102 ermittelten wichtigen IKT-Assets zu verwenden, zu installieren oder zu integrieren.	Artikel 103 Absatz 1 Risikominderungsmaßnahmen in der IKT-Lieferketten	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend
Die Kommission kann Durchführungsrechtsakte erlassen, um festzulegen, dass Einrichtungen der in den Anhängen I und II der Richtlinie (EU) 2022/2555 genannten Arten untersagt ist, von einer bestimmten Einrichtung bereitgestellte IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten	Artikel 103 Absatz 7	Erlass von Durchführungsrechtsakten	Konsultation der Mitgliedstaaten und der betreffenden Einrichtungen	Nicht zutreffend

enthalten, zu nutzen, zu installieren oder zu integrieren.				
Die Kommission erstellt im Wege von Durchführungsrechtsakten Listen von Hochrisikoanbietern, für die die mit Durchführungsrechtsakten gemäß Artikel 103 Absatz 1 erlassenen Verbote oder das Verbot gemäß Artikel 111 Absatz 1 relevant sind.	Artikel 104 Absatz 1	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend
Die Kommission kann Durchführungsrechtsakte erlassen, um die in Artikel 105 Absatz 2 Buchstabe b genannten Bedingungen weiter zu präzisieren und Durchführungsbestimmungen für die in Artikel 105 genannten Verfahren festzulegen.	Artikel 105 Ausnahmen für Einrichtungen, die in einem Drittland, für das Cybersicherheitsbedenken bestehen, niedergelassen sind oder die von in einem solchen Drittland niedergelassenen Einrichtungen kontrolliert werden	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend
Die Kommission kann Durchführungsrechtsakte mit Durchführungsbestimmungen über die Gebühren erlassen, in denen die Höhe der Gebühren und die Art und Weise ihrer Entrichtung präzisiert werden.	Artikel 109 Gebühren	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend
Die Kommission erlässt Durchführungsrechtsakte, um die Fristen für die schrittweise Entfernung der von Hochrisikoanbietern bereitgestellten IKT-Komponenten oder Komponenten, die entsprechende IKT-Komponenten enthalten, aus festen und	Artikel 110 Absatz 4 Wichtige IKT-Assets für mobile, feste und satellitengestützte elektronische Kommunikationsnetze	Erlass von Durchführungsrechtsakten	Nicht zutreffend	Nicht zutreffend

satellitengestützten elektronischen Kommunikationsnetzen festzulegen.				
Der Kommission kann gemäß Artikel 119 delegierte Rechtsakte zur Änderung des Anhangs II erlassen, um ihn unter Berücksichtigung der in Artikel 103 Absatz 3 genannten Elemente an die technologischen Entwicklungen anzupassen.	Artikel 110 Absatz 5	Erlass von delegierten Rechtsakten	Nicht zutreffend	Nicht zutreffend
7. Artikel 21 Absatz 5 wird wie folgt geändert: a) Unterabsatz 2 erhält folgende Fassung: „Die Kommission kann Durchführungsrechtsakte erlassen, in denen die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen in Bezug auf andere als die in Unterabsatz 1 genannten wesentlichen und wichtigen Einrichtungen festgelegt werden. Die Kommission bewertet regelmäßig, ob Durchführungsrechtsakte gemäß diesem Unterabsatz für bestimmte Sektoren oder Arten von Einrichtungen zu erlassen sind, um das Funktionieren des Binnenmarkts zu verbessern. Auf der Grundlage der Ergebnisse dieser	Artikel 1 Absatz 7, Richtlinie Maximale Harmonisierung	Die Kommission kann Durchführungsrechtsakte erlassen.		Nicht zutreffend

Bewertungen kann die Kommission solche Durchführungsrechtsakte für die ermittelten Sektoren oder Arten von Einrichtungen vorschlagen. Bei der Ausarbeitung solcher Bewertungen konzentriert sich die Kommission insbesondere auf den grenzübergreifenden Charakter von Sektoren oder Arten von Einrichtungen und führt ein offenes, transparentes und inklusives Konsultationsverfahren mit den einschlägigen Interessenträgern und den Mitgliedstaaten durch.“ b) Nach Unterabsatz 4 wird folgender Unterabsatz angefügt: „Erlässt die Kommission Durchführungsrechtsakte gemäß den Unterabsätzen 1 und 2, so erlegen die Mitgliedstaaten den in den Anwendungsbereich dieser Durchführungsrechtsakte fallenden Einrichtungen keine weiteren technischen oder methodischen Anforderungen an die in Artikel 21 Absatz 2 der Richtlinie (EU) 2022/2555 genannten Maßnahmen auf.“				

EUROPÄISCHE
KOMMISSION

Straßburg, den 20.1.2026
COM(2026) 11 final

ANNEXES 1 to 3

ANHÄNGE

des

Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates

über die Agentur der Europäischen Union für Cybersicherheit (ENISA), den europäischen Rahmen für die Cybersicherheitszertifizierung und die Sicherheit der IKT-Lieferketten sowie zur Aufhebung der Verordnung (EU) 2019/881 (Cybersicherheitsverordnung 2)

{SEC(2026) 11 final} - {SWD(2026) 11 final} - {SWD(2026) 12 final}

ANHANG I

ANFORDERUNGEN AN KONFORMITÄTSBEWERTUNGSSTELLEN

1. Eine Konformitätsbewertungsstelle muss nach nationalem Recht gegründet und mit Rechtspersönlichkeit ausgestattet sein.

2. Eine Konformitätsbewertungsstelle darf kein Hochrisikoanbieter sein.

3. Bei einer Konformitätsbewertungsstelle muss es sich um einen unabhängigen Dritten handeln, der mit der Einrichtung oder den IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten, die er bewertet, in keinerlei Verbindung steht. Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte, -Dienste oder -Prozesse oder verwaltete Sicherheitsdienste bewertet, an deren Entwurf, Herstellung, Bereitstellung, Montage, Verwendung oder Wartung Unternehmen beteiligt sind, die von diesem Verband vertreten werden, kann – sofern ihre Unabhängigkeit sowie die Abwesenheit von Interessenkonflikten nachgewiesen sind – als solcher Dritter gelten.

4. Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und das für die Erfüllung der Konformitätsbewertungsaufgaben zuständige Personal dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb der zu bewertenden IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste oder Einrichtungen, die sie bewerten, noch Bevollmächtigter einer dieser Parteien sein. Dies schließt nicht die Verwendung von bereits einer Bewertung unterzogenen IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste für persönliche Zwecke aus.

5. Eine Konformitätsbewertungsstelle, ihre oberste Leitungsebene und das für die Erfüllung der Konformitätsbewertungsaufgaben zuständige Personal dürfen weder direkt an Entwurf, Herstellung bzw. Bau, Vermarktung, Installation, Verwendung oder Instandsetzung dieser IKT-Produkte, -Dienste oder -Prozesse oder verwalteten Sicherheitsdienste oder Einrichtungen, die sie bewerten, beteiligt sein noch die an diesen Tätigkeiten beteiligten Parteien vertreten. Sie dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit ihren Konformitätsbewertungstätigkeiten beeinträchtigen können. Dies gilt insbesondere für Beratungsdienste.

6. Konformitätsbewertungsstellen müssen sicherstellen, dass die Tätigkeiten ihrer Zweigstellen oder Unterauftragnehmer die Vertraulichkeit, Objektivität oder Unparteilichkeit ihrer Konformitätsbewertungstätigkeiten nicht beeinträchtigen.

7. Falls eine Konformitätsbewertungsstelle Eigentum einer öffentlichen Stelle oder Einrichtung ist oder von dieser betrieben wird, sind die Unabhängigkeit und die Abwesenheit von Interessenkonflikten zwischen der nationalen Behörde für die Cybersicherheitszertifizierung und der Konformitätsbewertungsstelle sicherzustellen und zu dokumentieren.

8. Konformitätsbewertungsstellen und ihr Personal müssen die Konformitätsbewertungstätigkeiten mit höchster beruflicher Integrität und der erforderlichen fachlichen Kompetenz in dem betreffenden Bereich durchführen; sie dürfen keinerlei Einflussnahme durch Druck oder Vergünstigungen, insbesondere finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse

ihrer Konformitätsbewertungstätigkeiten auswirken könnte, insbesondere durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben.

9. Eine Konformitätsbewertungsstelle muss in der Lage sein, die bei der Konformitätsbewertung anfallenden Aufgaben, die ihr mit dieser Verordnung übertragen wurden, auszuführen, unabhängig davon, ob diese Aufgaben von ihr selbst oder in ihrem Namen und unter ihrer Verantwortung ausgeführt werden. Jegliche Unterauftragsvergabe oder die Inanspruchnahme von externem Personal ist angemessen zu dokumentieren, darf nicht über Vermittler erfolgen und bedarf einer schriftlichen Vereinbarung, in der unter anderem Vertraulichkeitsaspekte und Interessenkonflikte geklärt werden.

10. Eine Konformitätsbewertungsstelle muss jederzeit, für jedes Konformitätsbewertungsverfahren und für jede Art, Kategorie und Unterkategorie von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder Einrichtungen über Folgendes verfügen:

   a) das erforderliche Personal mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;

   b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt wird, wobei die Transparenz und Wiederholbarkeit der Verfahren sichergestellt werden; die Konformitätsbewertungsstelle muss über angemessene Regelungen und Verfahren verfügen, bei denen zwischen den Aufgaben, die sie als nach Artikel 93 notifizierte Stelle wahrnimmt, und ihren anderen Tätigkeiten unterschieden wird;

   c) Verfahren zur Durchführung von Tätigkeiten, bei denen die Größe eines Unternehmens, die Branche, in der es tätig ist, seine Struktur, der Grad an Komplexität der jeweiligen Technologie der IKT-Produkte, -Dienste oder -Prozesse und der Umstand, dass es sich um Massenfertigung oder Serienproduktion handelt, gebührend berücksichtigt werden.

11. Eine Konformitätsbewertungsstelle muss über die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben verfügen, die mit der Konformitätsbewertung verbunden sind, und Zugang zu allen benötigten Ausrüstungen und Einrichtungen haben.

12. Eine Konformitätsbewertungsstelle darf keine von Hochrisikoanbietern stammenden IKT-Komponenten oder Komponenten, die solche IKT-Komponenten enthalten, in wichtigen IKT-Assets gemäß Artikel 102 für Konformitätsbewertungstätigkeiten nach Titel III verwenden, diese installieren oder anderweitig integrieren.

13. Das Personal, das für die Durchführung von Konformitätsbewertungstätigkeiten zuständig ist, muss Folgendes besitzen:

   a) eine solide Fach- und Berufsausbildung, die alle Tätigkeiten der Konformitätsbewertung umfasst, für die die Konformitätsbewertungsstelle akkreditiert und gegebenenfalls ermächtigt wurde;

   b) eine ausreichende Kenntnis der Anforderungen, die mit den durchzuführenden Konformitätsbewertungen verbunden sind, und die entsprechende Befugnis, solche Bewertungen durchzuführen;

c) angemessene Kenntnis und angemessenes Verständnis der geltenden Anforderungen und Normen sowie der einschlägigen Bestimmungen der Harmonisierungsrechtsvorschriften der Union und ihrer Durchführungsrechtsakte;

d) die Fähigkeit zur Erstellung von Bescheinigungen, Protokollen und Berichten als Nachweis für durchgeführte Konformitätsbewertungen.

14. Konformitätsbewertungsstellen, ihre oberste Leitungsebene und das für die Erfüllung der Konformitätsbewertungsaufgaben zuständige Personal sowie etwaige Unterauftragnehmer müssen unparteiisch sein.

15. Die Vergütung der obersten Leitungsebene und des für Bewertungen zuständigen Personals darf sich nicht nach der Anzahl der durchgeführten Konformitätsbewertungen oder deren Ergebnissen richten.

16. Konformitätsbewertungsstellen müssen eine Haftpflichtversicherung abschließen, sofern die Haftpflicht nicht aufgrund des nationalen Rechts vom ihrem Mitgliedstaat übernommen wird oder der Mitgliedstaat selbst unmittelbar für die Konformitätsbewertung verantwortlich ist.

17. Das Personal einer Konformitätsbewertungsstelle muss die berufliche Schweigepflicht in Bezug auf alle Informationen wahren, die es bei der Durchführung seiner Aufgaben nach dieser Verordnung oder nach etwaigen Durchführungsbestimmungen der Mitgliedstaaten zu dieser Verordnung erhalten hat, außer wenn eine Offenlegung aufgrund von Rechtsvorschriften der Union oder des Mitgliedstaats, denen diese Personen unterliegen, erforderlich ist und außer gegenüber den zuständigen Behörden der Mitgliedstaaten, in denen sie ihre Tätigkeiten ausüben. Eigentumsrechte sind zu schützen. Die Konformitätsbewertungsstelle muss über dokumentierte Verfahren verfügen, mit denen die Einhaltung dieser Nummer sichergestellt wird.

18. Konformitätsbewertungsstellen müssen ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter, verhältnismäßiger und angemessener Geschäftsbedingungen ausüben, wobei sie unnötige Belastungen für Wirtschaftsteilnehmer vermeiden sowie in Bezug auf Gebühren die Interessen von Kleinstunternehmen und kleinen und mittleren Unternehmen berücksichtigen.

19. Konformitätsbewertungsstellen, die Zertifikate ausstellen, müssen die Anforderungen der einschlägigen harmonisierten Normen im Sinne des Artikels 2 Nummer 9 der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Konformitätsbewertungsstellen, die die Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen oder verwalteten Sicherheitsdiensten oder der Cyberabwehr von Einrichtungen vornehmen, erfüllen.

20. Konformitätsbewertungsstellen, die Bewertungstätigkeiten durchführen, müssen die Anforderungen der einschlägigen harmonisierten Normen für die Akkreditierung von Konformitätsbewertungsstellen, die diese Tätigkeiten durchführen, erfüllen.

21. Vergibt eine Konformitätsbewertungsstelle bestimmte mit der Konformitätsbewertung verbundene Aufgaben an Unterauftragnehmer oder überträgt sie diese einer Zweigstelle, so stellt sie sicher, dass der Unterauftragnehmer oder die Zweigstelle die Anforderungen des Anhangs und gegebenenfalls zusätzliche oder besondere Anforderungen, die in einem europäischen System für die Cybersicherheitszertifizierung festgelegt sind, erfüllt. Die

Konformitätsbewertungsstelle unterrichtet die nationale Behörde für die Cybersicherheitszertifizierung entsprechend.

22. Konformitätsbewertungsstellen tragen die volle Verantwortung für die Arbeiten, die von Unterauftragnehmern oder Zweigstellen ausgeführt werden, unabhängig davon, wo diese niedergelassen sind.

23. Konformitätsbewertungsstellen dürfen ihre Tätigkeiten nur mit Zustimmung des Herstellers oder Anbieters an einen Unterauftragnehmer vergeben oder einer Zweigstelle übertragen.

24. Konformitätsbewertungsstellen halten die einschlägigen Unterlagen über die Bewertung der Qualifikation des Unterauftragnehmers oder der Zweigstelle und die von ihnen gemäß dieser Verordnung ausgeführten Arbeiten für die nationale Behörde für die Cybersicherheitszertifizierung bereit.

ANHANG II

Wichtige IKT-Assets für mobile, feste und satellitengestützte elektronische Kommunikationsnetze

Kritische Infrastruktur	Wichtige IKT-Assets
1. 5G-Netze für die elektronische Kommunikation (nicht eigenständig und eigenständig)	Kernnetzfunktionen von Mobilfunk-Kommunikationsnetzen
	Virtualisierung von Netzfunktionen (NFV), Verwaltung und Netzorchestrierung (MANO)
	Funkzugangsnetz
2. Feste elektronische Kommunikationsnetze	Kernnetzfunktionen von festen elektronischen Kommunikationsnetzen
	Netzmanagementsystem
	Transport- und Übertragungsnetz
	Zugangsnetz
3. Satellitengestützte elektronische Kommunikationsnetze	Kernnetzfunktionen von satellitengestützten elektronischen Kommunikationsnetzen
	Netzmanagementsystem
	Kryptografische Produkte zum Schutz von Telekommando/Telemetrie
	Bodenstationen und ergänzende Bodenstationen

ANHANG III

ENTSPRECHUNGSTABELLE

Verordnung (EU) 2019/881	Die vorliegende Verordnung
Artikel 1 Absatz 1	Artikel 1 Absatz 1
Artikel 1 Absatz 1 Unterabsatz 2	Artikel 1 Absatz 2
Artikel 1 Absatz 2	Artikel 1 Absatz 4
Artikel 2	Artikel 2
Artikel 3	Artikel 3
Artikel 4	Artikel 4
Artikel 5	Artikel 5
Artikel 6	Artikel 6
Artikel 7 Absatz 1	Artikel 10 Absatz 1
Artikel 7 Absatz 2	Artikel 68 Absätze 1 und 2
Artikel 7 Absatz 3	Artikel 10 Absatz 2
Artikel 7 Absatz 4 Unterabsatz 1 Buchstaben a bis d	Artikel 10 Absatz 4
Artikel 7 Absatz 4 Unterabsatz 2	Artikel 68 Absatz 3
Artikel 7 Absatz 5	Artikel 14 Absätze 3 bis 5
Artikel 7 Absatz 6	Artikel 11 Absatz 1 Buchstabe f und Absatz 5
Artikel 7 Absatz 7	Artikel 11, Artikel 10 Absatz 5
Artikel 8 Absatz 1	Artikel 17 Absätze 1 und 2
Artikel 8 Absatz 2	–
Artikel 8 Absatz 3	–
Artikel 8 Absatz 4	Artikel 17 Absatz 1 Buchstabe d
Artikel 8 Absatz 5	Artikel 18 Absatz 6
Artikel 8 Absatz 6	Artikel 18 Absatz 4

Artikel 8 Absatz 7	Artikel 8
Artikel 9 Buchstabe a	Artikel 11 Absatz 2 Buchstabe a
Artikel 9 Buchstabe b	Artikel 11 Absatz 2 Buchstabe c
Artikel 9 Buchstabe c	Artikel 5 Absatz 1 Buchstabe a
Artikel 9 Buchstabe d	–
Artikel 9 Buchstabe e	–
Artikel 10	Artikel 7
Artikel 11	–
Artikel 12	Artikel 9
Artikel 13	Artikel 24
Artikel 14	Artikel 25
Artikel 15	Artikel 28
Artikel 16	Artikel 26
Artikel 17	Artikel 27
Artikel 18	Artikel 29
Artikel 19	Artikel 30
Artikel 20	Artikel 32
Artikel 21	Artikel 35
Artikel 22	–
Artikel 23	–
Artikel 24	Artikel 44
Artikel 25	Artikel 52
Artikel 26	Artikel 53
Artikel 27	Artikel 54
Artikel 28	Artikel 55
Artikel 29	Artikel 45

Artikel 30	Artikel 46
Artikel 31	Artikel 48
Artikel 32	Artikel 50
Artikel 33	Artikel 51
Artikel 34	Artikel 56
Artikel 35	Artikel 57
Artikel 36	Artikel 31
Artikel 37	Artikel 59
Artikel 38	Artikel 60
Artikel 39	Artikel 64
Artikel 40	Artikel 65
Artikel 41	Artikel 66
Artikel 42 Absatz 1	Artikel 70 Absatz 1
Artikel 42 Absatz 2	Artikel 70 Absatz 4
Artikel 42 Absatz 3	Artikel 70 Absatz 2
Artikel 43	Artikel 67
Artikel 44	Artikel 62
Artikel 45	Artikel 63
Artikel 46 Absätze 1 und 2	Artikel 71 Absätze 1 und 2
Artikel 47	–
Artikel 48	Artikel 73 Absätze 1 und 2
Artikel 49 Absatz 1	Artikel 74 Absatz 1
Artikel 49 Absatz 2	–
Artikel 49 Absatz 3	Artikel 74 Absatz 4
Artikel 49 Absatz 4	Artikel 74 Absatz 2
Artikel 49 Absatz 5	Artikel 74 Absatz 3

Artikel 49 Absatz 6	Artikel 74 Absatz 5
Artikel 49 Absatz 7	Artikel 74 Absatz 9
Artikel 49 Absatz 8	Artikel 76 Absatz 1
Artikel 49a Absätze 1 bis 3	Artikel 72 Absätze 3 bis 5
Artikel 49a Absatz 4	–
Artikel 50	Artikel 79 Absätze 1 und 3
Artikel 51 und 51a	Artikel 80 Absatz 1
Artikel 52	Artikel 82 Absätze 1 bis 7 und 9
Artikel 53	Artikel 83
Artikel 54 Absätze 1 und 2	Artikel 81 Absätze 1 bis 4
Artikel 54 Absätze 3 und 4	Artikel 78 Absätze 1 und 3
Artikel 55 Absatz 1	Artikel 84 Absätze 1 und 2
Artikel 55 Absatz 2	Artikel 84 Absatz 3
Artikel 56 Absatz 1	Artikel 85 Absatz 1
Artikel 56 Absatz 2	Artikel 71 Absatz 3
Artikel 56 Absatz 3	–
Artikel 56 Absatz 4	Artikel 85 Absatz 2
Artikel 56 Absätze 5 bis 9	Artikel 84 Absätze 3, 4, 6, 8 und 9
Artikel 56 Absatz 10	Artikel 71 Absatz 4
Artikel 57	Artikel 86 Absätze 1 bis 4
Artikel 58	Artikel 88
Artikel 59	Artikel 89
Artikel 60 Absätze 1, 2 und 4	Artikel 91 Absätze 1 bis 3
Artikel 60 Absatz 3	Artikel 92 Absatz 1
Artikel 61 Absatz 1	Artikel 93 Absatz 1
Artikel 61 Absätze 2 bis 4	–

Artikel 61 Absatz 5	Artikel 93 Absatz 3
Artikel 62 Absätze 1, 2, 4 und 5	Artikel 90 Absätze 1 bis 4
Artikel 62 Absatz 3	–
Artikel 63 und 64	Artikel 96
Artikel 65	Artikel 97
Artikel 66	Artikel 118
Artikel 67	Artikel 120
Artikel 68	Artikel 121
Artikel 69	Artikel 122