►B 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)

(Text von Bedeutung für den EWR)

(ABl. L 333 vom 27.12.2022, S. 80)

Berichtigt durch:

►C1 Berichtigung, ABl. L 90206 vom 22.12.2023, S. 1 (2022/2555)

▼B

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)

(Text von Bedeutung für den EWR)

KAPITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand

(1) In dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

(2) Zu diesem Zweck wird in dieser Richtlinie Folgendes festgelegt:

a) die Pflicht für alle Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit (zentrale Anlaufstellen) und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten;

b) Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten für Einrichtungen der in den Anhang I oder II aufgeführten Arten sowie für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden;

c) Vorschriften und Pflichten zum Austausch von Cybersicherheitsinformationen;

d) Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten.

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche oder private Einrichtungen der in den Anhang I oder II genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben.

▼B

Artikel 3 Absatz 4 des Anhangs dieser Empfehlung gilt nicht für die Zwecke dieser Richtlinie.

(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen der in den Anhang I oder II genannten Art, wenn

a) die Dienste erbracht werden von:

   i) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;

   ii) Vertrauensdiensteanbietern;

   iii) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern;

b) es sich bei der Einrichtung in einem Mitgliedstaat um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;

c) sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

d) eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

e) die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist;

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung:

   i) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung der Zentralregierung ist oder

   ii) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung auf regionaler Ebene ist, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.

(3) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden.

▼B

(4) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen, die Domänennamenregistrierungsdienste erbringen.

(5) Die Mitgliedstaaten können vorsehen, dass diese Richtlinie Anwendung findet auf:

a) Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene;

b) Bildungseinrichtungen, insbesondere wenn sie kritische Forschungstätigkeiten durchführen.

(6) Diese Richtlinie lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis, andere wesentliche staatliche Funktionen zu schützen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

(7) Diese Richtlinie gilt nicht für Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten.

(8) Zu diesem Zweck können die Mitgliedstaaten bestimmte Einrichtungen, die in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung tätig sind, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, oder die Dienste ausschließlich für die in Absatz 7 dieses Artikels genannten Einrichtungen der öffentlichen Verwaltung erbringen, von den in Artikel 21 oder 23 festgelegten Verpflichtungen in Bezug auf diese Tätigkeiten oder Dienste ausnehmen. In solchen Fällen gelten die in Kapitel VII genannten Aufsichts- und Durchsetzungsmaßnahmen nicht für diese spezifischen Tätigkeiten oder Dienste. Wenn die Einrichtungen ausschließlich Tätigkeiten der in diesem Absatz genannten Art ausüben oder entsprechende Dienste erbringen, können die Mitgliedstaaten auch beschließen, diese Einrichtungen von den in den Artikeln 3 und 27 festgelegten Verpflichtungen auszunehmen.

(9) Die Absätze 7 und 8 finden keine Anwendung, wenn eine Einrichtung als Vertrauensdiensteanbieter auftritt.

(10) Diese Richtlinie gilt nicht für Einrichtungen, die die Mitgliedstaaten gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2022/2554 vom Anwendungsbereich der genannten Verordnung ausgenommen haben.

(11) Die in dieser Richtlinie festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

(12) Diese Richtlinie gilt unbeschadet der Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG, der Richtlinien 2011/93/EU ([1]) und 2013/40/EU ([2]) des Europäischen Parlaments und des Rates sowie der Richtlinie (EU) 2022/2557.

([1]) Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

([2]) Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates (ABl. L 218 vom 14.8.2013, S. 8).

▼B

(13) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union oder der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden im Einklang mit dieser Richtlinie nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs relevanten und angemessenen Umfang beschränkt. Beim Informationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der betreffenden kritischen Einrichtungen geschützt.

(14) Einrichtungen, die zuständige Behörden, die zentrale Anlaufstellen und die CSIRTs verarbeiten personenbezogene Daten, soweit dies für die Zwecke dieser Richtlinie erforderlich ist und im Einklang mit der Verordnung (EU) 2016/679, insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung.

Die Verarbeitung personenbezogener Daten gemäß dieser Richtlinie durch Anbieter öffentlicher elektronischer Kommunikationsnetze oder Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste erfolgt im Einklang mit dem Datenschutzrecht der Union und dem Unionsrecht zum Schutz der Privatsphäre, insbesondere der Richtlinie 2002/58/EG.

Artikel 3

Wesentliche und wichtige Einrichtungen

(1) Für die Zwecke dieser Richtlinie gelten als wesentliche Einrichtungen:

a) Einrichtungen der in Anhang I aufgeführten Art, die die in Artikel 2 Absatz 1 des Anhangs der Empfehlung 2003/361/EG genannten Schwellenwerte für mittlere Unternehmen überschreiten;

b) qualifizierte Vertrauensdiensteanbieter und Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter, unabhängig von ihrer Größe;

c) Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG genannten als mittlere Unternehmen gelten;

d) Einrichtungen der öffentlichen Verwaltung nach Artikel 2 Absatz 2 Buchstabe f Ziffer i;

e) sonstige Einrichtungen der in Anhang I oder II aufgeführten Art, die von einem Mitgliedstaat gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wesentliche Einrichtungen eingestuft werden;

f) Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden und die in Artikel 2 Absatz 3 der vorliegenden Richtlinie genannt werden;

g) sofern der Mitgliedstaat dies vorsieht, Einrichtungen, die von den Mitgliedstaaten vor dem 16. Januar 2023 gemäß der Richtlinie (EU) 2016/1148 oder nach nationalem Recht als Betreiber wesentlicher Dienste eingestuft wurden.

▼B

(2) Für die Zwecke dieser Richtlinie gelten Einrichtungen der in Anhang I oder II aufgeführten Art, die nicht als wesentliche Einrichtungen im Sinne von Absatz 1 des vorliegenden Artikels gelten, als wichtige Einrichtungen. Dies schließt Einrichtungen ein, die von den Mitgliedstaaten gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wichtige Einrichtungen eingestuft wurden.

(3) Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen. Die Mitgliedstaaten überprüfen diese Liste danach regelmäßig, mindestens jedoch alle zwei Jahre, und aktualisieren sie gegebenenfalls.

(4) Für die Zwecke der Erstellung der in Absatz 3 genannten Liste schreiben die Mitgliedstaaten vor, dass die jenem Absatz genannten Einrichtungen den zuständigen Behörden mindestens die folgenden Informationen übermitteln:

a) den Namen der Einrichtung,

b) die Anschrift und aktuellen Kontaktdaten, einschließlich der E-Mail-Adressen, IP-Adressbereiche und Telefonnummern,

c) gegebenenfalls den relevanten Sektor und Teilsektor gemäß Anhang I oder II sowie

d) gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie Dienste erbringen, die in den Anwendungsbereich dieser Richtlinie fallen.

Die in Absatz 3 genannten Einrichtungen teilen alle Änderungen der gemäß Unterabsatz 1 des vorliegenden Absatzes übermittelten Angaben unverzüglich mit, in jedem Fall jedoch innerhalb von zwei Wochen ab dem Zeitpunkt der Änderung.

Die Kommission stellt mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) unverzüglich Leitlinien und Vorlagen für die in diesem Absatz festgelegten Verpflichtungen bereit.

Die Mitgliedstaaten können nationale Mechanismen für die Registrierung von Einrichtungen einrichten.

(5) Bis zum 17. April 2025 und danach alle zwei Jahre teilen die zuständigen Behörden Folgendes mit:

a) der Kommission und der Kooperationsgruppe für jeden Sektor und Teilsektor gemäß Anhang I oder II die Anzahl der wesentlichen und wichtigen Einrichtungen, die gemäß Absatz 3 auf die Liste aufgenommen wurden, und

b) der Kommission sachdienliche Informationen über die Zahl der wesentlichen und wichtigen Einrichtungen, die gemäß Artikel 2 Absatz 2 Buchstaben b bis e ermittelt wurden, über den Sektor und den Teilsektor gemäß Anhang I oder II, zu dem sie gehören, über die Art der von ihnen erbrachten Dienste und über die Bestimmung unter denen in Artikel 2 Absatz 2 Buchstaben b bis e festgelegten Bestimmungen, auf deren Grundlage sie ermittelt wurden.

▼B

(6) Bis zum 17. April 2025 können die Mitgliedstaaten der Kommission auf Ersuchen der Kommission die Namen der wesentlichen und wichtigen Einrichtungen gemäß Absatz 5 Buchstabe b mitteilen.

Artikel 4

Sektorspezifische Rechtsakte der Union

(1) Wenn wesentliche oder wichtige Einrichtungen gemäß sektorspezifischen Rechtsakten der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder erhebliche Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie, einschließlich der Bestimmungen über Aufsicht und Durchsetzung in Kapitel VII, keine Anwendung auf solche Einrichtungen. Wenn die sektorspezifischen Rechtsakte der Union nicht für alle in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen eines bestimmten Sektors gelten, kommen die einschlägigen Bestimmungen dieser Richtlinie weiterhin für Einrichtungen zur Anwendung, die nicht unter diese sektorspezifischen Rechtsakte der Union fallen.

(2) Die in Absatz 1 dieses Artikels genannten Anforderungen gelten den in dieser Richtlinie festgelegten Verpflichtungen in ihrer Wirkung als gleichwertig, wenn

a) die Maßnahmen zum Cybersicherheitsrisikomanagement den in Artikel 21 Absätze 1 und 2 festgelegten Maßnahmen in ihrer Wirkung mindestens gleichwertig sind, oder

b) der sektorspezifische Rechtsakt der Union einen unmittelbaren — gegebenenfalls automatischen und direkten — Zugang zu den Meldungen von Sicherheitsvorfällen durch die CSIRTs, die zuständigen Behörden oder die zentralen Anlaufstellen gemäß dieser Richtlinie vorsieht und wenn die Anforderungen an die Meldung erheblicher Sicherheitsvorfälle in ihrer Wirkung mindestens den in Artikel 23 Absätze 1 bis 6 festgelegten gleichwertig sind.

(3) Die Kommission wird bis zum 17. Juli 2023 Leitlinien zur Klarstellung der Anwendung der Absätze 1 und 2 bereitstellen. Die Kommission überprüft diese Leitlinien regelmäßig. Bei der Ausarbeitung der Leitlinien berücksichtigt die Kommission alle Stellungnahmen der Kooperationsgruppe und der ENISA.

Artikel 5

Mindestharmonisierung

Diese Richtlinie hindert die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen.

Artikel 6

Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

▼B

1. „Netz- und Informationssystem“

   a) ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Nummer 1 der Richtlinie (EU) 2018/1972,

   b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder

   c) digitale Daten, die von den — in den Buchstaben a und b genannten — Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können;

3. „Cybersicherheit“ die Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2019/881;

4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten im Bereich der Cybersicherheit und der zu ihrer Verwirklichung erforderlichen Governance in diesem Mitgliedstaat;

5. „Beinahe-Vorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist;

6. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt;

7. „Cybersicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat;

8. „Bewältigung von Sicherheitsvorfällen“ alle Maßnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon;

▼B

9. „Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;

10. „Cyberbedrohung“ eine Cyberbedrohung im Sinne des Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

11. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht;

12. „IKT-Produkt“ ein IKT-Produkt im Sinne des Artikels 2 Nummer 12 der Verordnung (EU) 2019/881;

13. „IKT-Dienst“ bezeichnet einen IKT-Dienst im Sinne des Artikels 2 Nummer 13 der Verordnung (EU) 2019/881;

14. „IKT-Prozess“ einen IKT-Prozess im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/881;

15. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann;

16. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([3]);

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

18. „Internet-Knoten“ eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt;

19. „Domänennamensystem“ oder „DNS“ ein verteiltes hierarchisches Verzeichnissystem, das die Identifizierung von Diensten und Ressourcen im Internet ermöglicht und es Endnutzergeräten erlaubt, Internet-Routing- und Konnektivitätsdienste zu nutzen, um diese Dienste und Ressourcen zu erreichen;

([3]) 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).

▼B

20. „DNS-Diensteanbieter“ eine Einrichtung, die

    a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domänennamen anbietet oder

    b) autoritative Dienste zur Auflösung von Domänennamen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;

21. „Namenregister der Domäne oberster Stufe“ oder „TLD-Namenregister“ eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain — TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden;

22. „Einrichtung, die Domänennamen-Registrierungsdienste erbringt“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;

23. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([4]);

24. „Vertrauensdienst“ einen Vertrauensdienst im Sinne des Artikels 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;

25. „Vertrauensdiensteanbieter“ einen Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;

26. „qualifizierter Vertrauensdienst“ einen qualifizierten Vertrauensdienst im Sinne des Artikels 3 Nummer 17 der Verordnung (EU) Nr. 910/2014;

27. „qualifizierter Vertrauensdiensteanbieter“ einen qualifizierten Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;

28. „Online-Marktplatz“ einen digitalen Dienst im Sinne des Artikels 2 Buchstabe n der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates ([5]);

29. „Online-Suchmaschine“ eine Online-Suchmaschine im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates ([6]);

([4]) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

([5]) Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken von Unternehmen gegenüber Verbrauchern im Binnenmarkt und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken) (ABl. L 149 vom 11.6.2005, S. 22).

([6]) Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57).

▼B

30. „Cloud-Computing-Dienst“ einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind;

31. „Rechenzentrumsdienst“ einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;

32. „Inhaltszustellnetz“ bezeichnet ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder schnellen Zustellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern;

33. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;

34. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen, eines Anbieters verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der bzw. die nicht in der Union niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an die Einrichtung — hinsichtlich der Pflichten dieser Einrichtung gemäß dieser Richtlinie wenden kann;

35. „Einrichtung der öffentlichen Verwaltung“ eine als solche in einem Mitgliedstaat nach nationalem Recht anerkannte Einrichtung, ausgenommen Justiz, Parlamente und Zentralbanken, die die folgenden Kriterien erfüllt:

    a) sie wurde zu dem Zweck gegründet, im allgemeinen Interesse liegende Aufgaben zu erfüllen, und hat keinen gewerblichen oder kommerziellen Charakter,

    b) sie besitzt Rechtspersönlichkeit oder ist gesetzlich dazu befugt, im Namen einer anderen Einrichtung mit eigener Rechtspersönlichkeit zu handeln,

    c) sie wird überwiegend vom Staat, Gebietskörperschaften oder von anderen Körperschaften des öffentlichen Rechts finanziert, untersteht hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften oder verfügt über ein Verwaltungs-, Leitungs- bzw. Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Körperschaften des öffentlichen Rechts eingesetzt worden sind,

    d) sie ist befugt, an natürliche oder juristische Personen Verwaltungs- oder Regulierungsentscheidungen zu richten, die deren Rechte im grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr berühren;

▼B

36. „öffentliches elektronisches Kommunikationsnetz“ ein öffentliches elektronisches Kommunikationsnetz im Sinne von Artikel 2 Nummer 8 der Richtlinie (EU) 2018/1972;

37. „elektronischer Kommunikationsdienst“ einen elektronischen Kommunikationsdienst im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972;

38. „Einrichtung“ eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;

39. „Anbieter verwalteter Dienste“ eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt;

40. „Anbieter verwalteter Sicherheitsdienste“ einen Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;

41. „Forschungseinrichtung“ eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen, die jedoch Bildungseinrichtungen nicht einschließt.

KAPITEL II

KOORDINIERTE RAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 7

Nationale Cybersicherheitsstrategie

(1) Jeder Mitgliedstaat erlässt eine nationale Cybersicherheitsstrategie, die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält. Die nationale Cybersicherheitsstrategie muss Folgendes umfassen:

a) Ziele und Prioritäten der Cybersicherheitsstrategie des Mitgliedstaats, die insbesondere die in den Anhängen I und II aufgeführten Sektoren abdecken;

b) einen Steuerungsrahmen zur Verwirklichung der unter Buchstabe a dieses Absatzes genannten Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte umfasst;

c) einen Steuerungsrahmen, in dem die Aufgaben und Zuständigkeiten der jeweiligen Interessenträger auf nationaler Ebene klargestellt, die Zusammenarbeit und Koordinierung auf nationaler Ebene zwischen den nach dieser Richtlinie zuständigen Behörden, zentralen Anlaufstellen und CSIRTs sowie die Koordinierung und Zusammenarbeit zwischen diesen Stellen und nach sektorspezifischen Rechtsakten der Union zuständigen Behörden untermauert werden;

▼B

d) einen Mechanismus zur Ermittlung von relevanten Anlagen und eine Bewertung der Cybersicherheitsrisiken in diesem Mitgliedstaat;

e) die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktionsfähigkeit und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

f) eine Liste der verschiedenen Behörden und Interessenträger, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;

g) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den nach dieser Richtlinie zuständigen Behörden und den nach der Richtlinie (EU) 2022/2557 zuständigen Behörden zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle und für die Wahrnehmung von Aufsichtsaufgaben, soweit zutreffend;

h) einen Plan, einschließlich erforderlicher Maßnahmen, zur Steigerung des allgemeinen Grads der Sensibilisierung für Cybersicherheit bei den Bürgerinnen und Bürgern.

(2) Im Rahmen der nationalen Cybersicherheitsstrategie nehmen die Mitgliedstaaten insbesondere Konzepte an

a) für die Cybersicherheit in der Lieferkette für IKT-Produkte und IKT-Dienste, die von Einrichtungen für die Erbringung ihrer Dienste genutzt werden;

b) für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und IKT-Dienste bei der Vergabe öffentlicher Aufträge, einschließlich hinsichtlich der Zertifizierung der Cybersicherheit, der Verschlüsselung und der Nutzung quelloffener Cybersicherheitsprodukte;

c) für das Vorgehen bei Schwachstellen, das die Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen nach Artikel 12 Absatz 1 umfasst;

d) im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit, Integrität und Vertraulichkeit des öffentlichen Kerns des offenen Internets, erforderlichenfalls einschließlich der Cybersicherheit von Unterseekommunikationskabeln;

e) zur Förderung der Entwicklung und Integration einschlägiger fortgeschrittener Technologien, damit Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf dem neuesten Stand zur Anwendung gelangen;

f) zur Förderung und Entwicklung der allgemeinen und beruflichen Bildung im Bereich der Cybersicherheit, von Kompetenzen, Sensibilisierungsmaßnahmen und Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit sowie der Anleitung zu guten Vorgehensweisen und Kontrollen im Bereich der Cyberhygiene für Bürgerinnen und Bürger, Interessenträger und Einrichtungen;

g) zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung, der Verbesserung des Einsatzes von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;

▼B

h) mit einschlägigen Verfahren und geeigneten Instrumenten für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheits-Informationen zwischen Einrichtungen im Einklang mit dem Unionsrecht zu unterstützen;

i) zur Stärkung des Grundniveaus für Cyberresilienz und Cyberhygiene kleiner und mittlerer Unternehmen, insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU, durch Bereitstellung leicht zugänglicher Orientierungshilfen und Unterstützung für ihre spezifischen Bedürfnisse;

j) zur Förderung eines aktiven Cyberschutzes.

(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrem Erlass. Die Mitgliedstaaten können auf ihre nationale Sicherheit bezogene Informationen von diesen Notifizierungen ausnehmen.

(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien regelmäßig, mindestens aber alle fünf Jahre auf der Grundlage wesentlicher Leistungsindikatoren und aktualisieren diese erforderlichenfalls. Die ENISA unterstützt die Mitgliedstaaten auf deren Wunsch bei der Entwicklung oder Aktualisierung einer nationalen Cybersicherheitsstrategie und wesentlicher Leistungsindikatoren für die Bewertung dieser Strategie, um sie mit den in dieser Richtlinie festgelegten Anforderungen und Verpflichtungen in Einklang zu bringen.

Artikel 8

Zuständige Behörden und zentrale Anlaufstellen

(1) Jeder Mitgliedstaat benennt eine oder mehrere für die Cybersicherheit und die in Kapitel VII genannten Aufsichtsaufgaben zuständige Behörden (zuständige Behörden) oder richtet sie ein.

(2) Die zuständigen Behörden gemäß Absatz 1 überwachen die Anwendung dieser Richtlinie auf nationaler Ebene.

(3) Jeder Mitgliedstaat benennt eine zentrale Anlaufstelle oder richtet sie ein. Benennt ein Mitgliedstaat nur eine zuständige Behörde nach Absatz 1 oder richtet er nur eine solche zuständige Behörde ein, so ist diese zuständige Behörde auch die zentrale Anlaufstelle dieses Mitgliedstaats.

(4) Jede zentrale Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit der Behörden des Mitgliedstaats mit den entsprechenden Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Kommission und der ENISA sowie die sektorübergreifende Zusammenarbeit mit anderen zuständigen Behörden innerhalb ihres Mitgliedstaats zu gewährleisten.

(5) Die Mitgliedstaaten gewährleisten, dass ihre zuständigen Behörden und zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können und die Ziele dieser Richtlinie somit erreicht werden.

(6) Die Mitgliedstaaten notifizieren der Kommission unverzüglich die Identität der zuständigen Behörde gemäß Absatz 1 und der zentralen Anlaufstelle gemäß Absatz 3, die Aufgaben dieser Behörden sowie etwaige spätere Änderungen dieser Angaben. Jeder Mitgliedstaat veröffentlicht die Identität seiner zuständigen Behörde. Die Kommission erstellt eine öffentlich verfügbare Liste der zentralen Anlaufstellen.

▼B

Artikel 9

Nationale Rahmen für das Cyberkrisenmanagement

(1) Jeder Mitgliedstaat benennt eine oder mehrere für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen zuständige Behörden (Behörden für das Cyberkrisenmanagement) oder richtet sie ein. Die Mitgliedstaaten stellen sicher, dass diese Behörden über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient ausführen zu können. Sie gewährleisten die Kohärenz mit den geltenden Rahmen für das allgemeine nationale Krisenmanagement.

(2) Benennt ein Mitgliedstaat mehr als eine Behörde für das Cyberkrisenmanagement im Sinne von Absatz 1 oder richtet mehr als eine solche zuständige Behörde ein, so gibt er eindeutig an, welche dieser zuständigen Behörden als Koordinator für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen fungiert.

(3) Jeder Mitgliedstaat ermittelt die Kapazitäten, Mittel und Verfahren, die im Fall einer Krise für die Zwecke dieser Richtlinie eingesetzt werden können.

(4) Jeder Mitgliedstaat verabschiedet einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen, in dem die Ziele und Modalitäten für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen festgelegt sind. In diesem Plan wird insbesondere Folgendes festgelegt:

a) die Ziele der nationalen Vorsorgenmaßnahmen und -tätigkeiten;

b) die Aufgaben und Zuständigkeiten der Behörden für das Cyberkrisenmanagement;

c) die Verfahren für das Cyberkrisenmanagement, einschließlich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und die Kanäle für den Informationsaustausch;

d) die nationalen Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen;

e) die einschlägigen öffentlichen und privaten Interessenträger und die betroffene Infrastruktur,

f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf Unionsebene beteiligen und dieses unterstützen kann.

(5) Spätestens drei Monate nach der Benennung oder Einrichtung der in Absatz 1 genannten Behörde für das Cyberkrisenmanagement meldet jeder Mitgliedstaat der Kommission die Identität seiner Behörde und eventueller späterer Änderungen daran. Die Mitgliedstaaten übermitteln der Kommission und dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) einschlägige die Anforderungen nach Absatz 4 betreffende Informationen über ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen innerhalb von drei Monaten nach dem Erlass dieser Pläne. Die Mitgliedstaaten können Informationen ausnehmen, wenn und soweit dies für ihre nationale Sicherheit erforderlich ist.

▼B

Artikel 10

Computer-Notfallteams (CSIRTs)

(1) Jeder Mitgliedstaat benennt ein oder mehrere CSIRTs oder richtet sie ein. Die CSIRTs können innerhalb einer zuständigen Behörde benannt oder eingerichtet werden. Die CSIRTs erfüllen die in Artikel 11 Absatz 1 festgelegten Anforderungen, decken mindestens die in den Anhängen I und II genannten Sektoren, Teilsektoren und Arten von Einrichtungen ab und sind für die Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf zuständig.

(2) Die Mitgliedstaaten gewährleisten, dass jedes CSIRT mit angemessenen Ressourcen ausgestattet ist, damit es seine in Artikel 11 Absatz 3 aufgeführten Aufgaben wirksam erfüllen kann.

(3) Die Mitgliedstaaten stellen sicher, dass jedes CSIRT über eine geeignete, sichere und belastbare Kommunikations- und Informationsinfrastruktur verfügt, über die es Informationen mit wesentlichen und wichtigen Einrichtungen und anderen einschlägigen Interessenträgern austauscht. Zu diesem Zweck stellen die Mitgliedstaaten sicher, dass jedes CSIRT zur Einführung sicherer Instrumente für den Informationsaustausch beiträgt.

(4) Die CSIRTs arbeiten mit sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen zusammen und tauschen mit diesen gemäß Artikel 29 gegebenenfalls einschlägige Informationen aus.

(5) Die CSIRTs nehmen an gemäß Artikel 19 organisierten Peer Reviews teil.

(6) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs in dem CSIRTs-Netzwerk wirksam, effizient und sicher zusammenarbeiten.

(7) Die CSIRTs können Kooperationsbeziehungen mit nationalen Computer-Notfallteams von Drittländern aufnehmen. Als Teil solcher Kooperationsbeziehungen erleichtern die Mitgliedstaaten den wirksamen, effizienten und sicheren Informationsaustausch mit diesen nationalen Computer-Notfallteams von Drittländern, wobei sie einschlägige Protokolle für den Informationsaustausch, einschließlich des Traffic Light Protocol, verwendet. Die CSIRTs können mit nationalen Computer-Notfallteams von Drittländern einschlägige Informationen, einschließlich personenbezogener Daten im Einklang mit dem Datenschutzrecht der Union, austauschen.

(8) Die CSIRTS können mit nationalen Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern kooperieren, insbesondere um Unterstützung im Bereich der Cybersicherheit zu leisten.

(9) Jeder Mitgliedstaat notifiziert der Kommission unverzüglich die Identität des CSIRT gemäß Absatz 1 und des als Koordinator gemäß Absatz 12 Absatz 1 benannten CSIRT, ihre jeweiligen Aufgaben in Bezug auf wesentliche und wichtige Einrichtungen sowie etwaige spätere Änderungen dieser Angaben.

(10) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Einsetzung ihrer CSIRTs ersuchen.

▼B

Artikel 11

Anforderungen an die CSIRTs sowie technische Kapazitäten und Aufgaben der CSIRTs

(1) Die CSIRTs müssen den folgenden Anforderungen genügen:

a) Die CSIRTs sorgen für einen hohen Grad der Verfügbarkeit ihrer Kommunikationskanäle, indem sie punktuellen Ausfällen vorbeugen und mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst mit anderen Kontakt aufnehmen können; sie legen die Kommunikationskanäle genau fest und machen sie den CSIRT-Nutzern und Kooperationspartnern bekannt;

b) die Räumlichkeiten der CSIRTs und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet;

c) die CSIRTs müssen über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, insbesondere um wirksame und effiziente Übergaben zu erleichtern;

d) die CSIRTs stellen die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeiten sicher;

e) die CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft ihrer Dienste gewährleisten können, und sie müssen sicherstellen, dass ihr Personal entsprechend geschult ist;

f) die CSIRTs müssen über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die Kontinuität ihrer Dienste sicherzustellen.

Die CSIRTs können sich an internationalen Kooperationsnetzen beteiligen.

(2) Die Mitgliedstaaten gewährleisten, dass ihre CSIRTs gemeinsam über die notwendigen technischen Fähigkeiten verfügen, damit sie ihre in Absatz 3 aufgeführten Aufgaben erfüllen können. Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs mit ausreichenden Ressourcen ausgestattet sind, um für angemessene Personalausstattungen zu sorgen, damit die CSIRTs ihre technischen Fähigkeiten entwickeln können.

(3) Die CSIRTs haben folgende Aufgaben:

a) Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene und auf Anfrage Bereitstellung von Unterstützung für betreffende wesentliche und wichtige Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit;

b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie an die zuständigen Behörden und andere einschlägige Interessenträger, möglichst echtzeitnah;

c) Reaktion auf Sicherheitsvorfälle und gegebenenfalls Unterstützung der betreffenden wesentlichen und wichtigen Einrichtungen;

▼B

d) Erhebung und Analyse forensischer Daten sowie dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit;

e) auf Ersuchen einer wesentlichen oder wichtigen Einrichtung eine proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung auf Schwachstellen mit potenziell signifikanten Auswirkungen (Schwachstellenscan);

f) Beteiligung am CSIRTs-Netzwerk und — im Rahmen ihrer Kapazitäten und Kompetenzen — auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks auf deren Ersuchen.

g) gegebenenfalls die Wahrnehmung der Aufgabe eines Koordinators für die Zwecke einer koordinierten Offenlegung von Schwachstellen nach Artikel 12 Absatz 1;

h) Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch gemäß Artikel 10 Absatz 3.

CSIRTs können eine proaktive nicht intrusive Überprüfung öffentlich zugänglicher Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen durchführen. Eine solche Überprüfung wird durchgeführt, um anfällige oder unsicher konfigurierte Netz- und Informationssysteme zu ermitteln und die betreffenden Einrichtungen zu unterrichten. Eine solche Überprüfung darf keinerlei nachteilige Auswirkung auf das Funktionieren der Dienste der Einrichtung haben.

Bei der Durchführung der in Unterabsatz 1 genannten Aufgaben können die CSIRTs auf der Grundlage eines risikobasierten Ansatzes bestimmten Aufgaben Vorrang einräumen.

(4) Die CSIRTs bauen Kooperationsbeziehungen mit einschlägigen Interessenträgern des Privatsektors auf, um die Ziele dieser Richtlinie erreichen zu können.

(5) Zur Erleichterung der Zusammenarbeit nach Absatz 4 fördern die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für

a) Verfahren zur Bewältigung von Sicherheitsvorfällen,

b) das Krisenmanagement und

c) die koordinierte Offenlegung von Schwachstellen nach Artikel 12 Absatz 1.

Artikel 12

Koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank

(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das als Koordinator benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder IKT-Dienste auf Ersuchen einer der beiden Seiten. Zu den Aufgaben des als Koordinator benannten CSIRT gehört insbesondere

▼B

a) betreffende Einrichtungen zu ermitteln und zu kontaktieren,

b) die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen, und

c) Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen.

Die Mitgliedstaaten stellen sicher, dass natürliche oder juristische Personen dem als Koordinator benannten CSIRT eine Schwachstelle, auf Wunsch anonym, melden können. Das als Koordinator benannte CSIRT stellt sicher, dass in Bezug auf die gemeldete Schwachstelle sorgfältige Folgemaßnahmen durchgeführt werden, und sorgen für die Anonymität der die Schwachstelle meldenden natürlichen oder juristischen Person. Wenn die gemeldete Schwachstelle erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten haben könnte, arbeitet das als Koordinator benannte CSIRT jedes betreffenden Mitgliedstaats gegebenenfalls mit den anderen als Koordinatoren benannten CSIRTs innerhalb des CSIRTs-Netzwerks zusammen.

(2) Die ENISA entwickelt und pflegt nach Absprache mit der Kooperationsgruppe eine europäische Schwachstellendatenbank. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein, pflegt diese und trifft die erforderlichen technischen und organisatorischen Maßnahmen, um die Sicherheit und Integrität der europäischen Schwachstellendatenbank zu gewährleisten, damit insbesondere Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, und deren Anbieter von Netz- und Informationssystemen auf freiwilliger Basis öffentlich bekannte Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können. Allen Interessenträgern wird Zugang zu den Informationen über die Schwachstellen gewährt, die in der europäischen Schwachstellendatenbank enthalten sind. Diese Datenbank umfasst Folgendes:

a) Informationen zur Beschreibung der Schwachstelle,

b) die betroffenen IKT-Produkte oder IKT-Dienste und das Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann,

c) die Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches von den zuständigen Behörden oder den CSIRTs bereitgestellte Orientierungshilfen für die Nutzer gefährdeter IKT-Produkte und IKT-Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.

Artikel 13

Zusammenarbeit auf nationaler Ebene

(1) Handelt es sich bei den zuständigen Behörden, der zentralen Anlaufstelle und den CSIRTs eines Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie bei der Erfüllung der in dieser Richtlinie festgelegten Pflichten zusammen.

▼B

(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von erheblichen Sicherheitsvorfällen gemäß Artikel 23 und Sicherheitsvorfällen, Cyberbedrohungen und Beinahe-Vorfällen gemäß Artikel 30 ihren CSIRTs oder gegebenenfalls ihren zuständigen Behörden übermittelt werden.

(3) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs oder gegebenenfalls zuständigen Behörden ihre zentralen Anlaufstellen über gemäß dieser Richtlinie vorgenommene Meldungen von Sicherheitsvorfällen, Cyberbedrohungen und Beinahe-Vorfällen unterrichten.

(4) Damit die Aufgaben und Pflichten der zuständigen Behörden, zentralen Anlaufstellen und CSIRTs wirksam erfüllt werden, sorgen die Mitgliedstaaten so weit wie möglich für eine angemessene Zusammenarbeit zwischen diesen Stellen und den Strafverfolgungsbehörden, den Datenschutzbehörden, den nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 und (EU) 2018/1139, den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014, den gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972, den gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden.

(5) Die Mitgliedstaaten stellen sicher, dass ihre im Rahmen dieser Richtlinie zuständigen Behörden und ihre nach der Richtlinie (EU) 2022/2557 zuständigen Behörden regelmäßig hinsichtlich der Identifizierung kritischer Einrichtungen zu Risiken, Cyberbedrohungen und Sicherheitsvorfällen sowie zu nicht cyberbezogenen Risiken, Bedrohungen und Sicherheitsvorfällen, die als kritische Einrichtungen im Sinne der Richtlinie (EU) 2022/2557 ermittelte wesentliche Einrichtungen betreffen, und zu den als Reaktion auf diese Risiken, Bedrohungen und Sicherheitsvorfälle ergriffenen Maßnahmen zusammenarbeiten und darüber Informationen austauschen. Die Mitgliedstaaten stellen ferner sicher, dass ihre im Rahmen dieser Richtlinie zuständigen Behörden und ihre nach der Verordnung (EU) Nr. 910/2014, der Verordnung (EU) 2022/2554 und der Richtlinie (EU) 2018/1972 zuständigen Behörden regelmäßig einschlägige Informationen austauschen, auch in Bezug auf einschlägige Sicherheitsvorfälle und Cyberbedrohungen.

(6) Die Mitgliedstaaten vereinfachen die Berichterstattung über die in den Artikeln 23 und 30 genannten technischen Mittel für Notifizierungen.

KAPITEL III

ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE

Artikel 14

Kooperationsgruppe

(1) Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten und zur Stärkung des Vertrauens wird eine Kooperationsgruppe eingesetzt.

(2) Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 7 wahr.

▼B

(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst nimmt an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) und die nach der Verordnung (EU) 2022/2554 zuständigen Behörden können sich gemäß Artikel 47 Absatz 1 jener Verordnung an den Tätigkeiten der Kooperationsgruppe beteiligen.

Gegebenenfalls kann die Kooperationsgruppe das Europäische Parlament und Vertreter der maßgeblichen Interessenträger einladen, an ihren Arbeiten teilzunehmen.

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(4) Die Kooperationsgruppe hat folgende Aufgaben:

a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie;

b) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Ausarbeitung und Durchführung von Maßnahmen zur koordinierten Offenlegung von Schwachstellen gemäß Artikel 7 Absatz 2 Buchstabe c;

c) Austausch bewährter Verfahren und Informationsaustausch im Zusammenhang mit der Durchführung dieser Richtlinie, auch in Bezug auf Cyberbedrohungen, Sicherheitsvorfälle, Schwachstellen, Beinahe-Vorfälle, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau, Normen und technische Spezifikationen sowie Bestimmung wesentlicher und wichtiger Einrichtungen gemäß Artikel 2 Absatz 2 Buchstaben b bis e;

d) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit und die allgemeine Kohärenz der sektorspezifischen Anforderungen an die Cybersicherheit;

e) beratender Austausch und Zusammenarbeit mit der Kommission bei Entwürfen von delegierten Rechtsakten oder Durchführungsrechtsakten, die gemäß dieser Richtlinie erlassen werden;

f) Austausch bewährter Verfahren und Informationsaustausch mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union;

g) Meinungsaustausch über die Durchführung sektorspezifischer Rechtsakte der Union, die Vorschriften über Cybersicherheit enthalten;

h) gegebenenfalls Erörterung von Berichten über die in Artikel 19 Absatz 9 genannten Peer-Reviews und Ausarbeitung von Schlussfolgerungen und Empfehlungen;

i) Durchführung koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1;

▼B

j) Erörterung von Fällen von Amtshilfe, einschließlich Erfahrungen und Ergebnisse gemeinsamer Aufsichtstätigkeiten in grenzübergreifenden Fällen gemäß Artikel 37;

k) auf Ersuchen eines oder mehrerer betreffender Mitgliedstaaten Erörterung spezifischer Amtshilfeersuchen gemäß Artikel 37;

l) Bereitstellung strategischer Orientierungshilfen für das CSIRTs-Netzwerk und das EU-CyCLONe zu spezifischen neu auftretenden Fragen;

m) Meinungsaustausch über das Konzept von Folgemaßnahmen im Anschluss an Cybersicherheitsvorfälle großen Ausmaßes und Krisen auf der Grundlage von im CSIRTs-Netzwerk und im EU-CyCLONe gewonnenen Erkenntnissen;

n) Beitrag zu den Cybersicherheitsfähigkeiten in der gesamten Union durch Erleichterung des Austauschs nationaler Bediensteter im Rahmen eines Programms zum Kapazitätsaufbau, an dem sich Mitarbeiter der zuständigen Behörden oder der CSIRTs beteiligen;

o) Organisation regelmäßiger gemeinsamer Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union, um die Tätigkeiten der Kooperationsgruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen;

p) Erörterung der Arbeiten im Zusammenhang mit Cybersicherheitsübungen, einschließlich der Arbeit der ENISA;

q) Festlegung der Methode und der organisatorischen Aspekte der Peer Reviews gemäß Artikel 19 Absatz 1 sowie Festlegung der Selbstbewertungsmethode für die Mitgliedstaaten gemäß Artikel 19 Absatz 5 mit der Unterstützung der Kommission und der ENISA und Entwicklung von Verhaltenskodizes zur Untermauerung der Arbeitsmethoden benannter Sachverständiger für Cybersicherheit gemäß Artikel 19 Absatz 6 in Zusammenarbeit mit der Kommission und der ENISA;

r) Ausarbeitung von Berichten über die auf strategischer Ebene und in den Peer Reviews gewonnenen Erfahrungen zum Zwecke der Überprüfung gemäß Artikel 40;

s) Erörterung und regelmäßige Bewertung des aktuellen Stands in Bezug auf Cyberbedrohungen oder Sicherheitsvorfälle wie Ransomware.

Die Kooperationsgruppe unterbreitet die in Unterabsatz 1 Buchstabe r genannten Berichte der Kommission, dem Europäischen Parlament und dem Rat.

(5) Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit ihrer Vertreter in der Kooperationsgruppe sicher.

(6) Die Kooperationsgruppe kann das CSIRTs-Netzwerk um einen technischen Bericht zu ausgewählten Themen ersuchen.

(7) Bis spätestens 1. Februar 2024 und danach alle zwei Jahre erstellt die Kooperationsgruppe ein Arbeitsprogramm bezüglich der Maßnahmen, die zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen sind.

▼B

(8) Die Kommission kann Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten erlassen, die für das Funktionieren der Kooperationsgruppe erforderlich sind.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Die Kommission tauscht sich mit der Kooperationsgruppe gemäß Absatz 4 Buchstabe e über die in den Unterabsatz 1 dieses Absatzes genannten Entwürfe von Durchführungsrechtsakten aus und arbeitet mit ihr zusammen.

(9) Die Kooperationsgruppe tagt regelmäßig und in jedem Fall mindestens einmal jährlich gemeinsam mit der mit der Richtlinie (EU) 2022/2557 eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch zu fördern und zu erleichtern.

Artikel 15

CSIRTs-Netzwerk

(1) Um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zwischen ihnen zu fördern, wird ein Netzwerk nationaler CSIRTs errichtet.

(2) Das CSIRTs-Netzwerk setzt sich aus Vertretern der gemäß Artikel 10 benannten oder eingerichteten CSIRTs der Mitgliedstaaten und des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) zusammen. Die Kommission nimmt als Beobachterin am CSIRTs-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und leistet aktive Unterstützung für die Zusammenarbeit zwischen den CSIRTs.

(3) Das CSIRTs-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Kapazitäten der CSIRTs;

b) Erleichterung der gemeinsamen Nutzung, des Transfers und des Austauschs von Technologie sowie relevanten Maßnahmen, Strategien, Instrumenten, Abläufen, bewährten Verfahren und Rahmenbedingungen zwischen den CSIRTs;

c) Austausch relevanter Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen;

d) Austausch von Informationen über Veröffentlichungen und Empfehlungen im Bereich Cybersicherheit;

e) Sicherstellung der Interoperabilität in Bezug auf Spezifikationen und Protokolle für den Informationsaustausch;

f) auf Antrag eines potenziell von einem Sicherheitsvorfall betroffenen Mitglieds des CSIRTs-Netzwerks Austausch und Erörterung von Informationen über diesen Sicherheitsvorfall und die damit verbundenen Cyberbedrohungen, Risiken und Schwachstellen;

g) auf Antrag eines Mitglieds des CSIRTs-Netzwerks Erörterung und, sofern möglich, Umsetzung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet seines Mitgliedstaats festgestellt wurde;

▼B

h) Unterstützung der Mitgliedstaaten bei der Bewältigung grenzübergreifender Sicherheitsvorfälle gemäß dieser Richtlinie;

i) Zusammenarbeit, Austausch bewährter Verfahren und Unterstützung der gemäß Artikel 12 Absatz 1 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;

j) Erörterung und Bestimmung weiterer Formen der operativen Zusammenarbeit, unter anderem im Zusammenhang mit

   i) Kategorien von Cyberbedrohungen und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

   iv) Grundsätzen und Modalitäten der Koordinierung bei der Reaktion auf grenzüberschreitende Risiken und Sicherheitsvorfälle,

   v) dem auf Ersuchen eines Mitgliedstaats erfolgenden Beitrag zum nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4;

k) Unterrichtung der Kooperationsgruppe über seine Tätigkeiten und über die gemäß Buchstabe j erörterten weiteren Formen der operativen Zusammenarbeit und gegebenenfalls Ersuchen um Orientierungshilfen dafür;

l) Berücksichtigung von Erkenntnissen aus Cybersicherheitsübungen, einschließlich der von der ENISA organisierten Übungen;

m) auf Antrag eines einzelnen CSIRT Erörterung der Kapazitäten und der Vorsorge dieses CSIRT;

n) Zusammenarbeit und Informationsaustausch mit regionalen und unionsweiten Sicherheitsbetriebszentren (Security Operations Centres), um die gemeinsame Lageerfassung bei Sicherheitsvorfällen und Cyberbedrohungen in der gesamten Union zu verbessern;

o) gegebenenfalls Erörterung der in Artikel 19 Absatz 9 genannten Peer Reviews;

p) Bereitstellung von Leitlinien zur Erleichterung der Konvergenz der operativen Verfahrensweisen in Bezug auf die Anwendung der die operative Zusammenarbeit betreffenden Bestimmungen dieses Artikels.

(4) Bis zum 17. Januar 2025 und danach alle zwei Jahre bewertet das CSIRTs-Netzwerk zum Zwecke der in Artikel 40 genannten Überprüfung den bei der operativen Zusammenarbeit erzielten Fortschritt und nimmt einen Bericht an. Der Bericht enthält insbesondere Schlussfolgerungen und Empfehlungen auf der Grundlage der Peer Reviews gemäß Artikel 19, die in Bezug auf nationale CSIRTs durchgeführt werden. Dieser Bericht wird der Kooperationsgruppe übermittelt.

(5) Das CSIRTs-Netzwerk gibt sich eine Geschäftsordnung.

(6) Das CSIRTs-Netzwerk und das EU-CyCLONe einigen sich auf Verfahrensregeln und arbeiten auf deren Grundlage zusammen.

▼B

Artikel 16

Das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)

(1) Zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wird das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet.

(2) EU-CyCLONe setzt sich aus den Vertretern der Behörden der Mitgliedstaaten für das Cyberkrisenmanagement sowie in Fällen, in denen ein potenzieller oder andauernder Cybersicherheitsvorfall großen Ausmaßes erhebliche Auswirkungen auf unter den Anwendungsbereich dieser Richtlinie fallende Dienste und Tätigkeiten hat oder wahrscheinlich haben wird, der Kommission zusammen. In anderen Fällen nimmt die Kommission als Beobachterin an den Tätigkeiten des EU-CyCLONe teil.

Die ENISA führt die Sekretariatsgeschäfte des EU-CyCLONe, unterstützt den sicheren Informationsaustausch und stellt die Instrumente bereit, die für die Förderung der Zusammenarbeit zwischen den Mitgliedstaaten zur Gewährleistung eines sicheren Informationsaustauschs erforderlich sind.

Gegebenenfalls kann das EU-CyCLONe Vertreter der maßgeblichen Interessenträger einladen, an seinen Arbeiten als Beobachter teilzunehmen.

(3) Das EU-CyCLONe hat folgende Aufgaben:

a) Verbesserung der Vorsorge im Hinblick auf das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen;

b) Entwicklung einer gemeinsamen Lageerfassung für Cybersicherheitsvorfälle großen Ausmaßes und Krisen;

c) Bewertung der Folgen und Auswirkungen relevanter Cybersicherheitsvorfälle großen Ausmaßes und Krisen und Vorschläge für mögliche Abhilfemaßnahmen;

d) Koordinierung des Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen sowie Unterstützung der Entscheidungsfindung auf politischer Ebene in Bezug auf solche Sicherheitsvorfälle und Krisen;

e) auf Ersuchen eines betreffenden Mitgliedstaats die Erörterung nationaler Pläne für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4.

(4) Das EU-CyCLONe gibt sich eine Geschäftsordnung.

(5) Das EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen sowie Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.

▼B

(6) Das EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten gemäß Artikel 15 Absatz 6 mit dem CSIRTs-Netzwerk zusammen.

(7) Bis zum 17. Juli 2024 und danach alle 18 Monate unterbreitet das EU-CyCLONe dem Europäischen Parlament und dem Rat einen Bericht, in dem es seine Arbeit bewertet.

Artikel 17

Internationale Zusammenarbeit

Die Union kann gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe, dem CSIRTs-Netzwerk und dem EU-CyCLONe ermöglicht und geregelt wird. Solche Übereinkünfte müssen mit dem Datenschutzrecht der Union im Einklang stehen.

Artikel 18

Bericht über den Stand der Cybersicherheit in der Union

(1) Die ENISA nimmt in Zusammenarbeit mit der Kommission und der Kooperationsgruppe einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union an und legt diesen Bericht dem Europäischen Parlament vor. Dieser Bericht wird unter anderem in maschinenlesbaren Daten zur Verfügung gestellt und muss Folgendes enthalten:

a) eine Bewertung der Cybersicherheitsrisiken auf Unionsebene unter Berücksichtigung der Cyberbedrohungslandschaft;

b) eine Bewertung der Entwicklung von Cybersicherheitskapazitäten im öffentlichen und im privaten Sektor in der gesamten Union;

c) eine Bewertung des allgemeinen Grads der Sensibilisierung für Cybersicherheit und der Cyberhygiene bei Bürgerinnen und Bürgern und Einrichtungen, einschließlich kleiner und mittlerer Unternehmen;

d) eine aggregierte Bewertung der Ergebnisse der Peer Reviews gemäß Artikel 19;

e) eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten und -ressourcen in der gesamten Union, einschließlich derjenigen auf Sektorenebene, sowie des Ausmaßes, in dem die nationalen Cybersicherheitsstrategien der Mitgliedstaaten aufeinander abgestimmt sind.

(2) Der Bericht muss insbesondere politische Empfehlungen zur Behebung von Mängeln und Erhöhung des Cybersicherheitsniveaus in der gesamten Union und eine Zusammenfassung der Ergebnisse der von der ENISA gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 für den entsprechenden Zeitraum erstellten technischen EU-Cybersicherheitslageberichte über Sicherheitsvorfälle und Cyberbedrohungen umfassen.

(3) Die ENISA entwickelt in Zusammenarbeit mit der Kommission, der Kooperationsgruppe und dem CSIRTs-Netzwerk die Methodik, einschließlich der einschlägigen Variablen wie quantitativer und qualitativer Indikatoren, für die in Absatz 1 Buchstabe e genannte aggregierte Bewertung.

▼B

Artikel 19

Peer Reviews

(1) Die Kooperationsgruppe wird bis zum 17. Januar 2025 mit Unterstützung der Kommission und der ENISA und gegebenenfalls des CSIRTs-Netzwerks die Methode und die organisatorischen Aspekte der Peer Reviews festlegen, um aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu stärken, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die für die Umsetzung dieser Richtlinie erforderlichen Cybersicherheitsfähigkeiten und -konzepte der Mitgliedstaaten zu verbessern. Die Teilnahme an Peer Reviews ist freiwillig. Die Peer Reviews werden von Sachverständigen für Cybersicherheit durchgeführt. Die Sachverständigen für Cybersicherheit werden von mindestens zwei Mitgliedstaaten benannt, die sich von dem überprüften Mitgliedstaat unterscheiden.

Die Peer Reviews erstrecken sich mindestens auf einen der folgenden Punkte:

a) den Stand der Umsetzung der Maßnahmen bezüglich Cybersicherheitsrisikomanagement und der Berichtspflichten gemäß den Artikeln 21 und 23;

b) das Niveau der Kapazitäten, einschließlich der verfügbaren finanziellen, technischen und personellen Ressourcen, und die Wirksamkeit bei der Durchführung der Aufgaben der zuständigen Behörden;

c) die operativen Kapazitäten der CSIRTs;

d) den Stand der Umsetzung der Amtshilfe gemäß Artikel 37;

e) den Stand der Umsetzung der Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Artikel 29;

f) spezifische Fragen mit grenz- oder sektorenübergreifendem Charakter.

(2) Die Methode muss gemäß Absatz 1 objektive, nichtdiskriminierende, faire und transparente Kriterien umfassen, anhand deren die Mitgliedstaaten Sachverständige für Cybersicherheit benennen, die für die Durchführung der Peer Reviews infrage kommen. Die ENISA und die Kommission nehmen als Beobachter an den Peer Reviews teil.

(3) Die Mitgliedstaaten können spezifische, in Absatz 1 Buchstabe f genannte Probleme für eine Peer Review ermitteln.

(4) Vor Beginn der Peer Review nach Absatz 1 teilen Mitgliedstaaten den teilnehmenden Mitgliedstaaten ihren Umfang, einschließlich der gemäß Absatz 3 ermittelten Probleme, mit.

(5) Vor Beginn der Peer Review können die Mitgliedstaaten eine Selbstbewertung der überprüften Aspekte vornehmen und diese Selbstbewertung den benannten Sachverständigen für Cybersicherheit vorlegen. Die Kooperationsgruppe legt mit Unterstützung der Kommission und der ENISA die Methode für die Selbstbewertung der Mitgliedstaaten fest.

▼B

(6) Die Peer Reviews umfassen physische oder virtuelle Besuche am Standort sowie abseits des Standorts den Austausch von Informationen. Im Einklang mit dem Grundsatz der guten Zusammenarbeit stellt der Mitgliedstaat, der Gegenstand der Peer Review ist, den benannten Sachverständigen für Cybersicherheit die für die Bewertung erforderlichen Informationen zur Verfügung, vorbehaltlich der Rechtsvorschriften der Union oder der Mitgliedstaaten über den Schutz vertraulicher oder als Verschlusssache eingestufter Informationen und der Wahrung grundlegender Funktionen des Staates wie der nationalen Sicherheit. Die Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission und der ENISA geeignete Verhaltenskodizes zur Untermauerung der Arbeitsmethoden der benannten Sachverständigen für Cybersicherheit. Sämtliche durch die Peer Review erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer Review beteiligten Sachverständigen für Cybersicherheit geben keine sensiblen oder vertraulichen Informationen, die im Laufe der Peer Review erlangt wurden, an Dritte weiter.

(7) Nachdem sie einer Peer Review unterzogen wurden, dürfen innerhalb von zwei Jahren nach Abschluss der Peer Review in diesem Mitgliedstaat keine weiteren Peer Reviews zu denselben Aspekten, die in einem Mitgliedstaat überprüft wurden, durchgeführt werden, es sei denn, der Mitgliedstaat beantragt etwas anderes oder es wird auf Vorschlag der Kooperationsgruppe etwas anderes vereinbart.

(8) Die Mitgliedstaaten stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen für Cybersicherheit den anderen Mitgliedstaaten, der Kooperationsgruppe, der Kommission und der ENISA vor Beginn der Peer Review offengelegt wird. Der Mitgliedstaat, der Gegenstand der Peer Review ist, kann Einwände gegen die Benennung bestimmter Sachverständiger für Cybersicherheit erheben, wenn er dem benennenden Mitgliedstaat stichhaltige Gründe mitteilt.

(9) Die an Peer Reviews beteiligten Sachverständigen für Cybersicherheit erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. Die einer Peer Review unterliegenden Mitgliedstaaten können zu den sie betreffenden Berichtsentwürfen Stellung nehmen; diese Stellungnahmen werden den Berichten beigefügt. Die Berichte enthalten Empfehlungen zur Verbesserung der im Rahmen der Peer Review behandelten Aspekte. Die Berichte werden gegebenenfalls der Kooperationsgruppe und dem CSIRTs-Netzwerk vorgelegt. Ein einer Peer Review unterliegender Mitgliedstaat kann beschließen, seinen Bericht oder eine redigierte Fassung davon öffentlich zugänglich zu machen.

KAPITEL IV

RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT

Artikel 20

Governance

(1) Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Die Anwendung dieses Absatzes lässt die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

▼B

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Artikel 21

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um 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.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

▼B

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d des vorliegenden Artikels die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen. Die Mitgliedstaaten stellen ferner sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach jenem Buchstaben die Ergebnisse der gemäß Artikel 22 Absatz 1 durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten berücksichtigen müssen.

(4) Die Mitgliedstaaten stellen sicher, dass eine Einrichtung, die feststellt, dass sie den in Absatz 2 genannten Maßnahmen nicht nachkommt, unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen ergreift.

(5) Bis zum 17. Oktober 2024 erlässt die Kommission Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter.

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 des vorliegenden Absatzes genannten wesentlichen und wichtigen Einrichtungen festgelegt werden.

Bei der Ausarbeitung der in den Unterabsätzen 1 und 2 des vorliegenden Absatzes genannten Durchführungsrechtsakte orientiert sich die Kommission so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen. Die Kommission tauscht sich mit der Kooperationsgruppe und der ENISA über die Entwürfe von Durchführungsrechtsakten gemäß Artikel 14 Absatz 4 Buchstabe e aus und arbeitet mit ihnen zusammen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 22

Koordinierte Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union

(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.

▼B

(2) Die Kommission legt nach Konsultation der Kooperationsgruppe und der ENISA sowie gegebenenfalls einschlägiger Interessenträger fest, welche spezifischen kritischen IKT-Dienste, -Systeme oder -Produkte der koordinierten Risikobewertung in Bezug auf die Sicherheit nach Absatz 1 unterzogen werden können

Artikel 23

Berichtspflichten

(1) Jeder Mitgliedstaat stellt sicher, dass wesentliche und wichtige Einrichtungen ihrem CSIRT oder gegebenenfalls ihrer zuständigen Behörde gemäß Absatz 4 unverzüglich über jeden Sicherheitsvorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste gemäß Absatz 3 (erheblicher Sicherheitsvorfall) hat. Gegebenenfalls unterrichten die betreffenden Einrichtungen die Empfänger ihrer Dienste unverzüglich über diese erheblichen Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Jeder Mitgliedstaat stellt sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es dem CSIRT oder gegebenenfalls der zuständigen Behörde ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat. Mit der bloßen Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.

Melden die betreffenden Einrichtungen der zuständigen Behörde einen erheblichen Sicherheitsvorfall gemäß Unterabsatz 1, so stellt der Mitgliedstaat sicher, dass diese zuständige Behörde die Meldung nach Eingang an das CSIRT weiterleitet.

Im Falle eines grenz- oder sektorenübergreifenden erheblichen Sicherheitsvorfalls stellen die Mitgliedstaaten sicher, dass ihre zentralen Anlaufstellen rechtzeitig einschlägige Informationen erhalten, die gemäß Absatz 4 gemeldet wurden.

(2) Gegebenenfalls stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die erhebliche Cyberbedrohung selbst.

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

a) er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;

b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

(4) Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln:

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

▼B

b) unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die unter Buchstabe a genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

c) auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde einen Zwischenbericht über relevante Statusaktualisierungen;

d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, der Folgendes enthält:

   i) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

   ii) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

   iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

   iv) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;

e) im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Buchstabe d stellen die Mitgliedstaaten sicher, dass die betreffenden Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls vorlegen.

Abweichend von Unterabsatz 1 Buchstabe b unterrichtet ein Vertrauensdiensteanbieter das CSIRT oder gegebenenfalls die zuständige Behörde in Bezug auf erhebliche Sicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls.

(5) Das CSIRT oder die zuständige Behörde übermitteln der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung gemäß Absatz 4 Buchstabe a eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operativer Beratung für die Durchführung möglicher Abhilfemaßnahmen. Ist das CSIRT nicht der ursprüngliche Empfänger der in Absatz 1 genannten Meldung, werden die Orientierungshilfen von der zuständigen Behörde in Zusammenarbeit mit dem CSIRT bereitgestellt. Das CSIRT leistet auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung. Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, gibt das CSIRT oder die zuständige Behörde ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

(6) Gegebenenfalls und insbesondere, wenn der erhebliche Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle unverzüglich die anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Sicherheitsvorfall. Diese Informationen umfassen die Art der gemäß Absatz 4 erhaltenen Informationen. Dabei wahren das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle im Einklang mit dem Unionsrecht oder dem einzelstaatlichen Recht die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

▼B

(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das CSIRT eines Mitgliedstaats oder gegebenenfalls seine zuständige Behörde sowie gegebenenfalls die CSIRTs oder die zuständigen Behörden anderer betreffender Mitgliedstaaten nach Konsultation der betreffenden Einrichtung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.

(8) Auf Ersuchen des CSIRT oder der zuständigen Behörde leitet die zentrale Anlaufstelle die nach Absatz 1 eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

(9) Die zentrale Anlaufstelle legt der ENISA alle drei Monate einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß Absatz 1 des vorliegenden Artikels und Artikel 30 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben verabschieden. Die ENISA unterrichtet die Kooperationsgruppe und das CSIRTs-Netzwerk alle sechs Monate über ihre Erkenntnisse zu den eingegangenen Meldungen.

(10) Die CSIRTs oder gegebenenfalls die zuständigen Behörden stellen den gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden Informationen über erhebliche Sicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung, die nach Absatz 1 des vorliegenden Artikels und Artikel 30 von Einrichtungen, die im Sinne der Richtlinie (EU) 2022/2557 als kritische Einrichtungen gelten, gemeldet wurden.

(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß Absatz 1 dieses Artikels und Artikel 30 sowie einer gemäß Absatz 2 dieses Artikels übermittelten Mitteilung näher bestimmt werden.

Bis zum 17. Oktober 2024 erlässt die Kommission in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke Durchführungsrechtsakte, in denen näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne von Absatz 3 anzusehen ist. Die Kommission kann solche Durchführungsrechtsakte in Bezug auf andere wesentliche und wichtige Einrichtungen erlassen.

Die Kommission tauscht sich mit der Kooperationsgruppe gemäß Artikel 14 Absatz 4 Buchstabe e über die in den Unterabsätzen 1 und 2 dieses Absatzes genannten Entwürfe von Durchführungsrechtsakten aus und arbeitet mit ihr zusammen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

▼B

Artikel 24

Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Die Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in Artikel 21 genannter Anforderungen nachzuweisen. Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen.

(2) Die Kommission ist befugt, gemäß Artikel 38 delegierte Rechtsakte zu erlassen, um diese Richtlinie dadurch zu ergänzen, dass ausgeführt wird, welche Kategorien wesentlicher und wichtiger Einrichtungen verpflichtet sind, bestimmte zertifizierte IKT-Produkte, -Dienste und -Prozesse zu nutzen oder ein Zertifikat im Rahmen eines gemäß Artikel 49 der Verordnung (EU) 2019/881 erlassenen europäischen Schemas für die Cybersicherheitszertifizierung zu erlangen. Diese delegierten Rechtsakte werden erlassen, wenn ein unzureichendes Niveau der Cybersicherheit festgestellt wurde, und umfassen eine Umsetzungsfrist.

Vor dem Erlass solcher delegierten Rechtsakte nimmt die Kommission eine Folgenabschätzung vor und führt Konsultationen gemäß Artikel 56 der Verordnung (EU) 2019/881 durch.

(3) Steht kein geeignetes europäisches Schema für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 dieses Artikels zur Verfügung, kann die Kommission nach Anhörung der Kooperationsgruppe und der Europäischen Gruppe für die Cybersicherheitszertifizierung die ENISA auffordern, ein mögliches Schema gemäß Artikel 48 Absatz 2 der Verordnung (EU) 2019/881 auszuarbeiten.

Artikel 25

Normung

(1) Um die einheitliche Anwendung des Artikels 21 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

(2) In Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls nach Konsultation einschlägiger Interessenträger bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen —, mit denen diese Bereiche abgedeckt werden könnten.

KAPITEL V

ZUSTÄNDIGKEIT UND REGISTRIERUNG

Artikel 26

Zuständigkeit und Territorialität

(1) Einrichtungen, die in den Anwendungsbereich dieser Richtlinie fallen, gelten als der Zuständigkeit des Mitgliedstaats unterliegend, in dem sie niedergelassen sind, außer in folgenden Fällen:

▼B

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, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, 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, der sie gegründet hat.

(2) Für die Zwecke dieser Richtlinie 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 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 in Absatz 1 Buchstabe b genannte Einrichtung 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. Wurde in der Union kein Vertreter im Sinne dieses Absatzes benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Richtlinie 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 Rechtshilfeersuchen 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, die in ihrem Hoheitsgebiet Dienste anbietet oder ein Netz- und Informationssystem betreibt.

Artikel 27

Register der Einrichtungen

(1) Die ENISA erstellt und pflegt ein Register der DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, 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 auf

▼B

der Grundlage der Informationen, die sie von den zentralen Anlaufstellen im Einklang mit Artikel 4 erhalten hat. Auf Ersuchen ermöglicht die ENISA den zuständigen Behörden den Zugang zu diesem Register, wobei sie gegebenenfalls für den Schutz der Vertraulichkeit der Informationen sorgt.

(2) Die Mitgliedstaaten verlangen von den in Absatz 1 genannten Einrichtungen, dass sie bis zum 17. Januar 2025 den zuständigen Behörden folgende Angaben übermitteln:

a) Name der Einrichtung,

b) gegebenenfalls, einschlägiger Sektor, Teilsektor und Art der Einrichtung gemäß Anhang I oder II,

c) Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen ist, Anschrift ihres nach Artikel 26 Absatz 3 benannten Vertreters,

d) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und gegebenenfalls ihres gemäß Artikel 26 Absatz 3 benannten Vertreters,

e) die Mitgliedstaaten, in denen die Einrichtung Dienste erbringt, und

f) die IP-Adressbereiche der Einrichtung.

(3) Die Mitgliedstaaten stellen sicher, dass im Falle einer Änderung der gemäß Absatz 2 übermittelten Angaben die in Absatz 1 genannten Einrichtungen die zuständige Behörde unverzüglich über diese Änderung, in jedem Fall aber innerhalb von drei Monaten ab dem Tag der Änderung, unterrichten.

(4) Nach Erhalt der in Absatz 2 und 3 genannten Angaben, mit Ausnahme der in Absatz 2 Buchstabe f genannten Angaben, leitet die zentrale Anlaufstelle des betreffenden Mitgliedstaats diese unverzüglich an die ENISA weiter.

(5) Gegebenenfalls werden die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Angaben über den in Artikel 3 Absatz 4 Unterabsatz 4 genannten nationalen Mechanismus übermittelt.

Artikel 28

Datenbank der Domänennamen-Registrierungsdaten

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, verpflichten die Mitgliedstaaten, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt sammeln und pflegen.

(2) Für die Zwecke des Absatzes 1 schreiben die Mitgliedstaaten vor, dass die Datenbank der Domänennamen-Registrierungsdaten die erforderlichen Angaben enthält, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. Diese Informationen müssen Folgendes umfassen:

▼B

a) den Domänennamen;

b) das Datum der Registrierung;

c) den Namen des Domäneninhabers, seine E-Mail-Adresse und Telefonnummer;

d) die Kontakt-E-Mail-Adresse und die Telefonnummer der Anlaufstelle, die den Domänennamen verwaltet, falls diese sich von denen des Domäneninhabers unterscheiden.

(3) Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, über Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, verfügen, mit denen sichergestellt wird, dass die in Absatz 1 genannten Datenbanken genaue und vollständige Angaben enthalten. Die Mitgliedstaaten schreiben vor, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.

(4) Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänennamen-Registrierungsdaten öffentlich zugänglich machen.

(5) Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, alle Anträge auf Zugang unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang eines Antrags auf Zugang beantworten. Die Mitgliedstaaten schreiben vor, dass diese Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

(6) Die Einhaltung der in den Absätzen 1 bis 5 festgelegten Verpflichtungen darf nicht zu einer doppelten Erhebung von Domänennamen-Registrierungsdaten führen. Zu diesem Zweck schreiben die Mitgliedstaaten vor, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, miteinander zusammenarbeiten.

KAPITEL VI

INFORMATIONSAUSTAUSCH

Artikel 29

Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass in den Anwendungsbereich dieser Richtlinie fallende Einrichtungen und gegebenenfalls andere Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, auf freiwilliger Basis relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen, sofern

▼B

a) dieser Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, aufzudecken, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen;

b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden oder indem die gemeinsame Forschung im Bereich Cyberbedrohung zwischen öffentlichen und privaten Einrichtungen gefördert wird.

(2) Die Mitgliedstaaten stellen sicher, dass der Informationsaustausch innerhalb Gemeinschaften wesentlicher und wichtiger Einrichtungen und gegebenenfalls ihrer Lieferanten oder Dienstleister stattfindet. Dieser Austausch muss im Wege von Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit unter Beachtung des potenziell sensiblen Charakters der ausgetauschten Informationen erfolgen.

(3) Die Mitgliedstaaten erleichtern die Festlegung von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2 dieses Artikels. In solchen Vereinbarungen können operative Elemente, einschließlich der Nutzung spezieller IKT-Plattformen und Automatisierungsinstrumente, der Inhalt und die Bedingungen der Vereinbarungen über den Informationsaustausch bestimmt werden. Bei der Festlegung der Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen können die Mitgliedstaaten Bedingungen für die von den zuständigen Behörden oder CSIRTs bereitgestellten Informationen festlegen. Die Mitgliedstaaten bieten Unterstützung bei der Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 7 Absatz 2 Buchstabe h genannten Konzepten.

(4) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen die zuständigen Behörden beim Abschluss von in Absatz 2 genannten Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder gegebenenfalls über ihren Rücktritt von solchen Vereinbarungen unterrichten, sobald dieser wirksam wird.

(5) Die ENISA unterstützt den Abschluss von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2, indem sie bewährte Verfahren austauscht und Orientierungshilfen zur Verfügung stellt.

Artikel 30

Freiwillige Meldung relevanter Informationen

(1) Die Mitgliedstaaten stellen sicher, dass zusätzlich zu der Berichtspflicht nach Artikel 23 Meldungen den CSIRTs oder gegebenenfalls den zuständigen Behörden auf freiwilliger Basis übermittelt werden können, und zwar durch:

a) wesentliche und wichtige Einrichtungen in Bezug auf Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle;

▼B

b) andere als die in Buchstabe a genannten Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, in Bezug auf erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle.

(2) Die Mitgliedstaaten bearbeiten die in Absatz 1 des vorliegenden Artikels genannten Meldungen nach dem in Artikel 23 vorgesehenen Verfahren. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten.

Erforderlichenfalls übermitteln die CSIRTs und gegebenenfalls die zuständigen Behörden den zentralen Anlaufstellen die Informationen über die gemäß diesem Artikel eingegangenen Meldungen, wobei sie die Vertraulichkeit und den angemessenen Schutz der von der meldenden Einrichtung übermittelten Informationen sicherstellen. Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen die freiwilligen Meldungen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

KAPITEL VII

AUFSICHT UND DURCHSETZUNG

Artikel 31

Allgemeine Aspekte der Aufsicht und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung der Verpflichtungen aus dieser Richtlinie wirksam beaufsichtigen und die erforderlichen Maßnahmen treffen.

(2) Die Mitgliedstaaten können ihren zuständigen Behörden gestatten, Aufsichtsaufgaben zu priorisieren. Diese Priorisierung beruht auf einem risikobasierten Ansatz. Zu diesem Zweck können die zuständigen Behörden bei der Wahrnehmung ihrer in den Artikeln 32 und 33 aufgeführten Aufsichtsaufgaben Aufsichtsmethoden festlegen, die eine Priorisierung dieser Aufgaben auf der Grundlage eines risikobasierten Ansatzes ermöglichen.

(3) Unbeschadet der Zuständigkeiten und Aufgaben der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 arbeiten die zuständigen Behörden bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, eng mit den Aufsichtsbehörden gemäß jener Verordnung zusammen.

(4) Unbeschadet der nationalen rechtlichen und institutionellen Rahmenbedingungen stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden bei der Überwachung der Einhaltung dieser Richtlinie durch Einrichtungen der öffentlichen Verwaltung und bei der Verhängung von Durchsetzungsmaßnahmenbei Verstößen gegen diese Richtlinie über die geeigneten Befugnisse verfügen, um diese Aufgaben in operativer Unabhängigkeit von den beaufsichtigten Einrichtungen der öffentlichen Verwaltung wahrzunehmen. Die Mitgliedstaaten können entscheiden, ob diesen Einrichtungen im Einklang mit den nationalen rechtlichen und institutionellen Rahmenbedingungen geeignete, verhältnismäßige und wirksame Aufsichts- und Durchsetzungsmaßnahmen auferlegt werden.

▼B

Artikel 32

Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Aufsichts- bzw. Durchsetzungsmaßnahmen, die wesentlichen Einrichtungen in Bezug auf die in dieser Richtlinie festgelegten Verpflichtungen auferlegt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wesentliche Einrichtungen befugt sind, in Bezug auf diese Einrichtungen mindestens folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführten Stichprobenkontrollen;

b) regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

c) Ad-hoc-Prüfungen, einschließlich solcher, die aufgrund eines erheblichen Sicherheitsvorfalls oder Verstoßes gegen diese Richtlinie der wesentlichen Einrichtung gerechtfertigt sind;

d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung;

e) Anforderung von Informationen, die für die Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die zuständigen Behörden nach Artikel 27;

f) Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind;

g) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften Einrichtung durchgeführt werden, oder auf sonstige verfügbare risikobezogene Informationen.

Die Ergebnisse einer gezielten Sicherheitsprüfung sind der zuständigen Behörde zur Verfügung zu stellen. Die Kosten einer solchen gezielten Sicherheitsprüfung, die von einer unabhängigen Stelle durchgeführt wird, sind von der geprüften Einrichtung zu tragen, es sei denn, die zuständige Behörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstaben e, f oder g geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.

(4) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wesentliche Einrichtungen mindestens befugt sind,

▼B

a) Warnungen über Verstöße gegen diese Richtlinie durch die betreffenden Einrichtungen herauszugeben;

b) verbindliche Anweisungen zu erlassen, auch in Bezug auf Maßnahmen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind, sowie Fristen für die Durchführung dieser Maßnahmen und für die Berichterstattung über ihre Durchführung zu setzen, oder Anordnungen zu erlassen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen diese Richtlinie zu beheben;

c) die betreffenden Einrichtungen anzuweisen, das gegen diese Richtlinie verstoßende Verhalten einzustellen und von Wiederholungen abzusehen;

d) die betreffenden Einrichtungen anzuweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist sicherzustellen, dass ihre Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Artikel 21 im Einklang stehen, bzw. die in Artikel 23 festgelegten Berichtspflichten zu erfüllen;

e) die betreffenden Einrichtungen anzuweisen, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

f) die betreffenden Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung der Artikel 21 und 23 durch die betreffenden Einrichtungen überwacht;

h) die betreffenden Einrichtungen anzuweisen, Aspekte der Verstöße gegen diese Richtlinie entsprechend bestimmten Vorgaben öffentlich bekannt zu machen;

i) gemäß einzelstaatlichem Recht zusätzlich zu jeglichen der unter den Buchstaben a bis h dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 34 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Erweisen sich die gemäß Absatz 4 Buchstaben a bis d und f ergriffenen Durchsetzungsmaßnahmen als unwirksam, so stellen die Mitgliedstaaten sicher, dass ihre zuständigen Behörden befugt sind, eine Frist festzusetzen, innerhalb derer die wesentliche Einrichtung die erforderlichen Maßnahmen ergreifen muss, um die Mängel zu beheben oder die Anforderungen dieser Behörden zu erfüllen. Für den Fall, dass die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen werden, stellen die Mitgliedstaaten sicher, dass ihre zuständigen Behörden befugt sind,

a) die Zertifizierung oder Genehmigung für einen Teil oder alle von der wesentlichen Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten vorübergehend auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle oder ein Gericht im Einklang mit dem nationalen Recht aufzufordern, die Zertifizierung oder Genehmigung vorübergehend auszusetzen;

b) zu verlangen, dass die zuständigen Stellen oder Gerichte im Einklang mit dem nationalen Recht natürlichen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind, vorübergehend untersagen, Leitungsaufgaben in dieser Einrichtung wahrzunehmen.

▼B

Die gemäß diesem Absatz verhängten vorübergehenden Aussetzungen oder Verbote werden nur so lange angewandt, bis die betreffende Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Durchsetzungsmaßnahmenverhängt wurden, zu erfüllen. Für die Verhängung solcher vorübergehenden Aussetzungen oder Verbote muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, der Unschuldsvermutung und der Verteidigungsrechte, entsprechen.

Die in diesem Absatz vorgesehenen Durchsetzungsmaßnahmen finden keine Anwendung auf Einrichtungen der öffentlichen Verwaltung, die dieser Richtlinie unterliegen.

(6) Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu gewährleisten, dass die Einrichtung diese Richtlinie erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können.

Für Einrichtungen der öffentlichen Verwaltung gilt dieser Absatz unbeschadet der nationalen Rechtsvorschriften über die Haftung von öffentlichen Bediensteten und von gewählten oder ernannten Amtsträgern.

(7) Bei der Ergreifung von Durchsetzungsmaßnahmen gemäß Absatz 4 oder 5 müssen die zuständigen Behörden die Verteidigungsrechte einhalten und den Umständen des Einzelfalls Rechnung tragen und dabei zumindest Folgendes gebührend berücksichtigen:

a) die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde, wobei u. a. Folgendes immer als schwerer Verstoß anzusehen ist:

   i) wiederholte Verstöße,

   ii) eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen,

   iii) eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden,

   iv) die Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes von der zuständigen Behörde angeordnet wurden, sowie

   v) Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementmaßnahmen im Bereich der Cybersicherheit oder Berichtspflichten gemäß den Artikeln 21 und 23.

b) die Dauer des Verstoßes;

c) einschlägige frühere Verstöße der betreffenden Einrichtung;

d) der verursachte materielle oder immaterielle Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und die Zahl der betroffenen Nutzer;

▼B

e) etwaiger Vorsatz oder etwaige Fahrlässigkeit des Urhebers des Verstoßes;

f) von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens;

g) Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;

h) Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit den zuständigen Behörden.

(8) Die zuständigen Behörden müssen ihre Durchsetzungsmaßnahmen ausführlich begründen. Bevor sie solche Maßnahmen ergreifen, teilen die zuständigen Behörden den betreffenden Einrichtungen ihre vorläufigen Erkenntnisse mit. Sie räumen diesen Einrichtungen ferner eine angemessene Frist zur Stellungnahme ein, außer in hinreichend begründeten Fällen, in denen sofortige Maßnahmen zur Verhütung von Sicherheitsvorfällen oder zur Reaktion auf Sicherheitsvorfälle andernfalls beeinträchtigt würden.

(9) Die Mitgliedstaaten stellen sicher, dass ihre gemäß der vorliegenden Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse — mit denen sichergestellt werden soll, dass Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden, diese Richtlinie erfüllen — die gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden innerhalb desselben Mitgliedstaats unterrichten. Gegebenenfalls können die gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden die gemäß der vorliegenden Richtlinie zuständigen Behörden ersuchen, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine Einrichtung, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtung eingestuft wird, auszuüben.

(10) Die Mitgliedstaaten stellen sicher, dass ihre gemäß der vorliegenden Richtlinie zuständigen Behörden mit den gemäß der Verordnung (EU) 2022/2554 jeweils zuständigen Behörden des betreffenden Mitgliedstaats zusammenarbeiten. Insbesondere stellen die Mitgliedstaaten sicher, dass ihre gemäß dieser Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse — mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die als IKT-Drittanbieter gemäß Artikel 31 der Verordnung (EU) 2022/2554 benannt wurden, diese Richtlinie erfüllen — das gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2022/2554 eingerichtete Überwachungsforum unterrichten.

Artikel 33

Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wichtige Einrichtungen

(1) Werden Nachweise, Hinweise oder Informationen vorgelegt, wonach eine wichtige Einrichtung mutmaßlich dieser Richtlinie, insbesondere deren Artikeln 21 und 23, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden. Die Mitgliedstaaten stellen sicher, dass diese Maßnahmen wirksam, verhältnismäßig und abschreckend sind, wobei die Umstände des Einzelfalls jeweils zu berücksichtigen sind.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wichtige Einrichtungen befugt sind, in Bezug auf diese Einrichtungen mindestens folgende Maßnahmen vorzunehmen:

▼B

a) Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen, die von geschulten Fachkräften durchgeführt werden;

b) gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

c) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls auch in Zusammenarbeit mit der betreffenden Einrichtung;

d) Anforderung von Informationen, die für die nachträgliche Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die zuständigen Behörden nach Artikel 27;

e) Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind;

f) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von von einem qualifizierten Prüfer durchgeführten Sicherheitsprüfungen und der entsprechenden zugrunde liegenden Nachweise.

Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften Einrichtung durchgeführt werden, oder auf sonstige verfügbare risikobezogene Informationen.

Die Ergebnisse gezielter Sicherheitsprüfungen sind der zuständigen Behörde zur Verfügung zu stellen. Die Kosten einer solchen gezielten Sicherheitsprüfung, die von einer unabhängigen Stelle durchgeführt wird, sind von der geprüften Einrichtung zu tragen, es sei denn, die zuständige Behörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstabe d, e oder f geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.

(4) ►C1 Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wichtige Einrichtungen mindestens dazu befugt sind, ◄

a) Warnungen über Verstöße gegen diese Richtlinie durch die betreffenden Einrichtungen herauszugeben;

b) verbindliche Anweisungen oder Anordnungen zu erlassen, um die betreffenden Einrichtungen aufzufordern, die festgestellten Mängel oder den Verstoß gegen diese Richtlinie zu beheben;

c) die betreffenden Einrichtungen anzuweisen, das gegen diese Richtlinie verstoßende Verhalten einzustellen und von Wiederholungen abzusehen;

d) die betreffenden Einrichtungen anzuweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist sicherzustellen, dass ihre Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Artikel 21 im Einklang stehen, bzw. die in Artikel 23 festgelegten Berichtspflichten zu erfüllen;

▼B

e) die betreffenden Einrichtungen anzuweisen, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

f) die betreffenden Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) die betreffenden Einrichtungen anzuweisen, Aspekte der Verstöße gegen diese Richtlinie entsprechend bestimmten Vorgaben öffentlich bekannt zu machen;

h) gemäß einzelstaatlichem Recht zusätzlich zu jeglichen der unter den Buchstaben a bis g dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 34 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Artikel 32 Absätze 6, 7 und 8 gelten entsprechend für die Aufsichts- und Durchsetzungsmaßnahmen, die in diesem Artikel für wichtige Einrichtungen vorgesehen sind.

(6) Die Mitgliedstaaten stellen sicher, dass ihre gemäß der vorliegenden Richtlinie zuständigen Behörden mit den gemäß der Verordnung (EU) 2022/2554 jeweils zuständigen Behörden des betreffenden Mitgliedstaats zusammenarbeiten. Insbesondere stellen die Mitgliedstaaten sicher, dass ihre gemäß dieser Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse — mit denen sichergestellt werden soll, dass wichtige Einrichtungen, die als IKT-Drittanbieter gemäß Artikel 31 der Verordnung (EU) 2022/2554 benannt wurden, diese Richtlinie erfüllen — das gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2022/2554 eingerichtete Überwachungsforum unterrichten.

Artikel 34

Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Geldbußen, die gemäß dem vorliegenden Artikel gegen wesentliche und wichtige Einrichtungen in Bezug auf Verstöße gegen diese Richtlinie verhängt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

(2) Geldbußen werden zusätzlich zu jeglichen der Maßnahmen nach Artikel 32 Absatz 4 Buchstaben a bis h, Artikel 32 Absatz 5 und Artikel 33 Absatz 4 Buchstaben a bis g verhängt.

(3) Bei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 32 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

(4) Die Mitgliedstaaten stellen sicher, dass gegen wesentliche Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 10 000 000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

▼B

(5) Die Mitgliedstaaten stellen sicher, dass gegen wichtige Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 7 000 000 EUR oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(6) Die Mitgliedstaaten können die Befugnis vorsehen, Zwangsgelder zu verhängen, um eine wesentliche oder wichtige Einrichtung zu zwingen, einen Verstoß gegen diese Richtlinie gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen.

(7) Unbeschadet der Befugnisse der zuständigen Behörden gemäß den Artikeln 32 und 33 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung Geldbußen verhängt werden können.

(8) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, so stellt dieser Mitgliedstaat sicher, dass dieser Artikel so angewandt wird, dass die Geldbuße von der zuständigen Behörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von den zuständigen Behörden verhängten Geldbußen haben. In jedem Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Der betreffende Mitgliedstaat teilt der Kommission bis zum 17. Oktober 2024 die Rechtsvorschriften, die er aufgrund dieses Absatzes erlässt, sowie unverzüglich alle nachfolgenden Änderungsgesetze oder Änderungen dieser Vorschriften mit.

Artikel 35

Verstöße mit Verletzungen des Schutzes personenbezogener Daten

(1) Stellen die zuständigen Behörden im Zuge der Beaufsichtigung oder Durchsetzung fest, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 21 und 23 der vorliegenden Richtlinie festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie unverzüglich die in Artikel 55 oder 56 jener Verordnung genannten Aufsichtsbehörden.

(2) Verhängen die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden gemäß Artikel 58 Absatz 2 Buchstabe i der genannten Verordnung eine Geldbuße, so dürfen die zuständigen Behörden für einen Verstoß im Sinne von Absatz 1 des vorliegenden Artikels, der sich aus demselben Verhalten ergibt wie jener Verstoß, der Gegenstand der Geldbuße nach Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 war, keine Geldbuße nach Artikel 34 der vorliegenden Richtlinie verhängen. Die zuständigen Behörden können jedoch die Durchsetzungsmaßnahmen gemäß Artikel 32 Absatz 4 Buchstaben a bis h, Artikel 32 Absatz 5 und Artikel 33 Absatz 4 Buchstaben a bis g dieser Richtlinie anwenden bzw. verhängen.

(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so setzt die zuständige Behörde die in ihrem eigenen Mitgliedstaat angesiedelte Aufsichtsbehörde über die mögliche Verletzung des Schutzes personenbezogener Daten nach Absatz 1 in Kenntnis.

▼B

Artikel 36

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Maßnahmen zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 17. Januar 2025 mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

Artikel 37

Amtshilfe

(1) Wenn eine Einrichtung ihre Dienste in mehr als einem Mitgliedstaat erbringt oder wenn sie ihre Dienste in einem oder mehreren Mitgliedstaaten erbringt und sich ihre Netz- und Informationssysteme in einem oder mehreren anderen Mitgliedstaaten befinden, so arbeiten die zuständigen Behörden der betreffenden Mitgliedstaaten zusammen und unterstützen einander. Diese Zusammenarbeit umfasst mindestens Folgendes:

a) über die zentralen Anlaufstellen unterrichten die zuständigen Behörden, die in einem Mitgliedstaat Aufsichts- oder Durchsetzungsmaßnahmen ergreifen, die zuständigen Behörden in den anderen betreffenden Mitgliedstaaten über die Aufsichts- und Durchsetzungsmaßnahmen und konsultieren sie zu diesen;

b) eine zuständige Behörde kann eine andere zuständige Behörde ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen;

c) auf begründetes Ersuchen einer anderen zuständigen Behörde leistet eine zuständige Behörde der ersuchenden Behörde in einem ihren zur Verfügung stehenden Ressourcen angemessenen Umfang Amtshilfe, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können.

Die in Unterabsatz 1 Buchstabe c genannte Amtshilfe kann 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 einen solchen Antrag ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden sowie — auf Ersuchen eines der betreffenden Mitgliedstaaten — die Kommission und die ENISA.

▼B

(2) Die zuständigen Behörden verschiedener Mitgliedstaaten können, wenn angezeigt und im gegenseitigen Einvernehmen, gemeinsame Aufsichtsmaßnahmen durchführen.

KAPITEL VIII

DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

Artikel 38

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 24 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 16. Januar 2023 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 24 Absatz 2 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 24 Absatz 2 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 39

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

▼B

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

(3) Wird die Stellungnahme des Ausschusses im schriftlichen Verfahren eingeholt, so wird das Verfahren ohne Ergebnis abgeschlossen, wenn der Vorsitz des Ausschusses dies innerhalb der Frist zur Abgabe der Stellungnahme beschließt oder ein Ausschussmitglied dies verlangt.

KAPITEL IX

SCHLUSSBESTIMMUNGEN

Artikel 40

Überprüfung

Bis zum 17. Oktober 2027 und danach alle 36 Monate überprüft die Kommission die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der Größe der betreffenden Einrichtungen, und der Sektoren, der Teilsektoren und der Arten der in den Anhängen I und II genannten Einrichtung für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewertet. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRTs-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Dem Bericht ist erforderlichenfalls ein Gesetzgebungsvorschlag beizufügen.

Artikel 41

Umsetzung

(1) Bis zum 17. Oktober 2024 erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Vorschriften ab dem 18. Oktober 2024 an.

(2) Bei Erlass der in Absatz 1 genannten Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

Artikel 42

Änderung der Verordnung (EU) Nr. 910/2014

In der Verordnung (EU) Nr. 910/2014 wird Artikel 19 mit Wirkung vom 18. Oktober 2024 gestrichen.

Artikel 43

Änderung der Richtlinie (EU) 2018/1972

In der Richtlinie (EU) 2018/1972 werden die Artikel 40 und 41 mit Wirkung vom 18. Oktober 2024 gestrichen.

▼B

Artikel 44

Aufhebung

Die Richtlinie (EU) 2016/1148 wird mit Wirkung vom 18. Oktober 2024 aufgehoben.

Bezugnahmen auf die durch die vorliegende Richtlinie aufgehobene Richtlinie gelten als Bezugnahmen auf die vorliegende Richtlinie und sind nach Maßgabe der Entsprechungstabelle in Anhang III zu lesen.

Artikel 45

Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Artikel 46

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

▼B

ANHANG I

SEKTOREN MIT HOHER KRITIKALITÄT

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates ([1]), die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne von Artikel 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944
		— Erzeuger im Sinne des Artikels 2 Nummer 38 der Richtlinie (EU) 2019/944
		— nominierte Strommarktbetreiber im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates ([2]) — Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten — Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters
	b) Fernwärme und -kälte	— Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates ([3])
	c) Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		— zentrale Bevorratungsstellen im Sinne des Artikels 2 Buchstabe f der Richtlinie 2009/119/EG des Rates ([4])
	d) Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates ([5])
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG
		— Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/73/EG
		— Betreiber einer Speicheranlage im Sinne des Artikels 2 Nummer 10 der Richtlinie 2009/73/EG

▼B

Sektor	Teilsektor	Art der Einrichtung
		— Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG
		— Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG
		— Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	e) Wasserstoff	— Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2. Verkehr	a) Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ([6]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates ([7]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		— Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates ([8]) bereitstellen
	b) Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ([9])
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 jener Richtlinie
	c) Schifffahrt	— Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates ([10]) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe

▼B

Sektor	Teilsektor	Art der Einrichtung
		— Leitungsorgane von Häfen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates ([11]), einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		— Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates ([12])
	d) Straßenverkehr	— Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ([13]), die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
		— Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates ([14])
3. Bankwesen		Kreditinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([15])
4. Finanzmarktinfrastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([16])
		— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([17])
5. Gesundheitswesen		— Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([18])
		— EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates ([19])
		— Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates ([20]) ausüben — Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen — Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates ([21]) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden

▼B

Sektor	Teilsektor	Art der Einrichtung
6. Trinkwasser		Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates ([22]), jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
7. Abwasser		Unternehmen, die kommunales Abwasser, häusliches Abwasser oder industrielles Abwasser im Sinne des Artikels 2 Nummern 1, 2 und 3 der Richtlinie 91/271/EWG des Rates ([23]) sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
8. Digitale Infrastruktur		— Betreiber von Internet-Knoten
		— DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern
		— TLD-Namenregister
		— Anbieter von Cloud-Computing-Diensten
		— Anbieter von Rechenzentrumsdiensten
		— Betreiber von Inhaltszustellnetzen
		— Vertrauensdiensteanbieter
		— Anbieter öffentlicher elektronischer Kommunikationsnetze oder
		— Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
9. Verwaltung von IKT-Diensten (Business-to-Business)		— Anbieter verwalteter Dienste — Anbieter verwalteter Sicherheitsdienste
10. öffentliche Verwaltung		— Einrichtungen der öffentlichen Verwaltung von Zentralregierungen entsprechend der Definition eines Mitgliedstaats gemäß nationalem Recht
		— Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene entsprechend der Definition eines Mitgliedstaats gemäß nationalem Recht

▼B

Sektor	Teilsektor	Art der Einrichtung
11. Weltraum		Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

([1]) Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125).
([2]) Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54).
([3]) Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen (ABl. L 328 vom 21.12.2018, S. 82).
([4]) Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten (ABl. L 265 vom 9.10.2009, S. 9).
([5]) Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG (ABl. L 211 vom 14.8.2009, S. 94).
([6]) Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11).
([7]) Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348 vom 20.12.2013, S. 1).
([8]) Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums („Rahmenverordnung“) (ABl. L 96 vom 31.3.2004, S. 1).
([9]) Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums (ABl. L 343 vom 14.12.2012, S. 32).
([10]) Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6).
([11]) Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28).
([12]) Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates vom 27. Juni 2002 über die Einrichtung eines gemeinschaftlichen Überwachungs- und Informationssystems für den Schiffsverkehr und zur Aufhebung der Richtlinie 93/75/EWG des Rates (ABl. L 208 vom 5.8.2002, S. 10).
([13]) Delegierte Verordnung (EU) 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste (ABl. L 157 vom 23.6.2015, S. 21).
([14]) Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern (ABl. L 207 vom 6.8.2010, S. 1).
([15]) Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).
([16]) Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. L 173 vom 12.6.2014, S. 349).
([17]) Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates vom 4. Juli 2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (ABl. L 201 vom 27.7.2012, S. 1).
([18]) Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45).
([19]) Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26).
([20]) Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel (ABl. L 311 vom 28.11.2001, S. 67).
([21]) Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1).
([22]) Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 435 vom 23.12.2020, S. 1).
([23]) Richtlinie 91/271/EWG des Rates vom 21. Mai 1991 über die Behandlung von kommunalem Abwasser (ABl. L 135 vom 30.5.1991, S. 40).

▼B

ANHANG II

SONSTIGE KRITISCHE SEKTOREN

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten im Sinne des Artikels 2 Nummer 1a der Richtlinie 97/67/EG, einschließlich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates ([1]), ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates ([2]), die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates ([3]), die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates ([4]) herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates ([5]) herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektrischen Ausrüstungen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

02022L2555 — DE — 27.12.2022 — 000.004 — 56

▼B

Sektor	Teilsektor	Art der Einrichtung
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6. Anbieter digitaler Dienste		— Anbieter von Online-Marktplätzen
		— Anbieter von Online-Suchmaschinen
		— Anbieter von Plattformen für Dienste sozialer Netzwerke
7. Forschung		Forschungseinrichtungen

([1]) Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über Abfälle und zur Aufhebung bestimmter Richtlinien (ABl. L 312 vom 22.11.2008, S. 3).
([2]) Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Chemikalienagentur, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission (ABl. L 396 vom 30.12.2006, S. 1).
([3]) Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1).
([4]) Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1).
([5]) Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176).

▼B

ANHANG III

ENTSPRECHUNGSTABELLE

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
Artikel 1 Absatz 1	Artikel 1 Absatz 1
Artikel 1 Absatz 2	Artikel 1 Absatz 2
Artikel 1 Absatz 3	—
Artikel 1 Absatz 4	Artikel 2 Absatz 12
Artikel 1 Absatz 5	Artikel 2 Absatz 13
Artikel 1 Absatz 6	Artikel 2 Absätze 6 und 11
Artikel 1 Absatz 7	Artikel 4
Artikel 2	Artikel 2 Absatz 14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	—
Artikel 6	—
Artikel 7 Absatz 1	Artikel 7 Absätze 1 und 2
Artikel 7 Absatz 2	Artikel 7 Absatz 4
Artikel 7 Absatz 3	Artikel 7 Absatz 3
Artikel 8 Absätze 1 bis 5	Artikel 8 Absätze 1 bis 5
Artikel 8 Absatz 6	Artikel 13 Absatz 4
Artikel 8 Absatz 7	Artikel 8 Absatz 6
Artikel 9 Absätze 1, 2 und 3	Artikel 10 Absätze 1, 2 und 3
Artikel 9 Absatz 4	Artikel 10 Absatz 9
Artikel 9 Absatz 5	Artikel 10 Absatz 10
Artikel 10 Absätze 1 und 2 und Absatz 3 Unterabsatz 1	Artikel 13 Absätze 1, 2 und 3
Artikel 10 Absatz 3 Unterabsatz 2	Artikel 23 Absatz 9
Artikel 11 Absatz 1	Artikel 14 Absätze 1 und 2
Artikel 11 Absatz 2	Artikel 14 Absatz 3
Artikel 11 Absatz 3	Artikel 14 Absatz 4 Unterabsatz 1 Buchstaben a bis q und Buchstabe s und Absatz 7

▼B

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
Artikel 11 Absatz 4	Artikel 14 Absatz 4 Unterabsatz 1 Buchstabe r und Unterabsatz 2
Artikel 11 Absatz 5	Artikel 14 Absatz 8
Artikel 12 Absätze 1 bis 5	Artikel 15 Absätze 1 bis 5
Artikel 13	Artikel 17
Artikel 14 Absätze 1 und 2	Artikel 21 Absätze 1 bis 4
Artikel 14 Absatz 3	Artikel 23 Absatz 1
Artikel 14 Absatz 4	Artikel 23 Absatz 3
Artikel 14 Absatz 5	Artikel 23 Absätze 5, 6 und 8
Artikel 14 Absatz 6	Artikel 23 Absatz 7
Artikel 14 Absatz 7	Artikel 23 Absatz 11
Artikel 15 Absatz 1	Artikel 31 Absatz 1
Artikel 15 Absatz 2 Unterabsatz 1 Buchstabe a	Artikel 32 Absatz 2 Buchstabe e
Artikel 15 Absatz 2 Unterabsatz 1 Buchstabe b	Artikel 32 Absatz 2 Buchstabe g
Artikel 15 Absatz 2 Unterabsatz 2	Artikel 32 Absatz 3
Artikel 15 Absatz 3	Artikel 32 Absatz 4 Buchstabe b
Artikel 15 Absatz 4	Artikel 31 Absatz 3
Artikel 16 Absätze 1 und 2	Artikel 21 Absätze 1 bis 4
Artikel 16 Absatz 3	Artikel 23 Absatz 1
Artikel 16 Absatz 4	Artikel 23 Absatz 3
Artikel 16 Absatz 5	—
Artikel 16 Absatz 6	Artikel 23 Absatz 6
Artikel 16 Absatz 7	Artikel 23 Absatz 7
Artikel 16 Absätze 8 und 9	Artikel 21 Absatz 5 und Artikel 23 Absatz 11
Artikel 16 Absatz 10	—
Artikel 16 Absatz 11	Artikel 2 Absätze 1, 2 und 3
Artikel 17 Absatz 1	Artikel 33 Absatz 1
Artikel 17 Absatz 2 Buchstabe a	Artikel 32 Absatz 2 Buchstabe e
Artikel 17 Absatz 2 Buchstabe b	Artikel 32 Absatz 4 Buchstaben b

▼B

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
Artikel 17 Absatz 3	Artikel 37 Absatz 1 Buchstaben a und b
Artikel 18 Absatz 1	Artikel 26 Absatz 1 Buchstabe b und Absatz 2
Artikel 18 Absatz 2	Artikel 26 Absatz 3
Artikel 18 Absatz 3	Artikel 26 Absatz 4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	—
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Anhang I Nummer 1	Artikel 11 Absatz 1
Anhang I Nummer 2 Buchstabe a Ziffern i bis iv	Artikel 11 Absatz 2 Buchstaben a bis d
Anhang I Nummer 2 Buchstabe a Ziffer v	Artikel 11 Absatz 2 Buchstabe f
Anhang I Nummer 2 Buchstabe b	Artikel 11 Absatz 4
Anhang I Nummer 2 Buchstabe c Ziffern i und ii	Artikel 11 Absatz 5 Buchstabe a
Anhang II	Anhang I
Anhang III Nummern 1 und 2	Anhang II Nummer 6
Anhang III Nummer 3	Anhang I Nummer 8