VERNEHMLASSUNGSBERICHT

DER REGIERUNG

BETREFFEND

DIE TOTALREVISION DES CYBER-SICHERHEITSGESETZES (CSG)

(Umsetzung der 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) sowie die Durchführung der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit))

Ministerium für Präsidiales und Finanzen

Vernehmlassungsfrist: 26. April 2024

INHALTSVERZEICHNIS

Beilagen:

- Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80-152);
- Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für

Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15-69);

- TOC – Umsetzung der Richtlinie (EU) 2022/2555.

ZUSAMMENFASSUNG

Mit der gegenständlichen Vorlage soll insbesondere die 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) ins liechtensteinische Recht umgesetzt werden.

Die 2016 eingeführten EU-Vorschriften zur Cybersicherheit – die Richtlinie (EU) 2016/1148, die im Fürstentum Liechtenstein mit dem Cyber-Sicherheitsgesetz (CSG) national umgesetzt wurde und am 1. Juli 2023 in Kraft trat – wurden Anfang 2023 durch die NIS-2-Richtlinie aktualisiert. Die NIS-2-Richtlinie modernisiert den bestehenden Rechtsrahmen, um mit der zunehmenden Digitalisierung und einer sich entwickelnden Bedrohungslandschaft für Cybersicherheit Schritt zu halten.

Wie bereits in der Richtlinie (EU) 2016/1148 vorgesehen, regelt die Richtlinie (EU) 2022/2555 vor allem die Pflicht für alle EWR-Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden, zuständige nationale Behörden und zentrale Anlaufstellen für Cybersicherheit sowie Computer-Notfallteams (CSIRTs) zu benennen oder einzurichten. Neu hinzu kommt die Pflicht zur Benennung und Einrichtung einer Behörde für das Cyberkrisenmanagement. Ebenso werden neue Begrifflichkeiten in Bezug auf das Cybersicherheitsrisikomanagement (Sicherheitsanforderungen) sowie der Berichtspflichten (Meldung von Sicherheitsvorfällen) eingeführt. Wesentlich ist auch die Ausweitung des Anwendungsbereichs auf weitere Sektoren und Teilsektoren, wodurch die Resilienz und Reaktionsfähigkeit öffentlicher und privater Einrichtungen, der zuständigen Behörden und des EWR insgesamt weiter verbessert werden. Die Richtlinie (EU) 2022/2555 findet beispielsweise Anwendung auf die zusätzlichen (Teil-)Sektoren Fernwärme und -kälte und Wasserstoff (Energie), Abwasser, Weltraum und die öffentliche Verwaltung sowie für Post- und Kurierdienste, Abfallbewirtschaftung, Produktion, Verarbeitung und Vertrieb von Lebensmitteln oder auch die Forschung.

Weiters soll mit der gegenständlichen Vorlage für eine Totalrevision des CSG die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit)

und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) durchgeführt werden.

Mit der Verordnung (EU) 2019/881 wird neben der ENISA ein europäischer Rahmen für die Cybersicherheitszertifizierung aufgebaut. Auf Grundlage dieses Rahmens werden in weiterer Folge die Anforderungen an die zu entwickelnden sogenannten europäischen Schemata für die Cybersicherheitszertifizierung festgelegt, damit die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen für IKT-Produkte, -Dienste oder -Prozesse in allen EWR-Mitgliedstaaten anerkannt und verwendet werden können.

Der europäische Rahmen für die Cybersicherheitszertifizierung soll in einheitlicher Weise in allen EWR-Mitgliedstaaten eingeführt werden. Damit soll es aufgrund gleicher Anforderungsniveaus in den EWR-Mitgliedstaaten zu keinem «Zertifizierungsshopping» kommen. Die Cybersicherheitszertifizierung spielt eine grosse Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und deren Sicherheit zu erhöhen.

ZUSTÄNDIGES MINISTERIUM

Ministerium für Präsidiales und Finanzen

BETROFFENE STELLEN

Amt für Bevölkerungsschutz
Amt für Kommunikation
Amt für Hochbau und Raumplanung
Amt für Informatik
Amt für Tiefbau und Geoinformation
Datenschutzstelle
Finanzmarktaufsicht
Landespolizei
Staatsanwaltschaft
Stabsstelle Cyber-Sicherheit
Stabsstelle FIU
Gemeinden

Öffentlich-rechtliche Stiftungen und Anstalten
Andere juristische Personen des öffentlichen und privaten Rechts, die überwiegend vom Staat, den Gemeinden oder von anderen Einrichtungen des öffentlichen Rechts finanziert werden oder deren Aufsicht unterliegen.

Vaduz, 6. Februar 2024

LNR 2024-66

P

1. AUSGANGSLAGE

Ziel der Richtlinie (EU) 2016/1148 (NIS-1-Richtlinie) war der Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen. Die NIS-1-Richtlinie wurde im Cyber-Sicherheitsgesetz (CSG) national umgesetzt. Das CSG trat am 1. Juli 2023 sowie die entsprechende Verordnung am 7. September 2023 in Kraft.

Eine Überprüfung der NIS-1-Richtlinie in der Europäischen Union (EU) hat jedoch Mängel aufgezeigt, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern. So wurde beispielsweise festgestellt, dass die EWR-Mitgliedstaaten die NIS-1-Richtlinie sehr unterschiedlich umsetzten, unter anderem in Bezug auf ihren Anwendungsbereich, dessen Abgrenzung weitgehend im Ermessen der EWR-Mitgliedstaaten lag. Auch wurde den EWR-Mitgliedstaaten ein sehr grosser Ermessensspielraum bei der Umsetzung der in der Richtlinie festgelegten Verpflichtungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen eingeräumt. Im Ergebnis führte dies zu einer Vielzahl sehr unterschiedlicher Regelungen auf nationaler Ebene und schliesslich zu einer unzureichenden Cyber-Resilienz von für die Gesellschaft und Wirtschaft wichtigen Unternehmen. So werden aktuell nicht alle kritischen Sektoren erfasst und es

existieren unterschiedliche Sicherheitsanforderungen und Meldepflichten zwischen den EWR-Mitgliedstaaten. Ebenso existieren eine schwach ausgeprägte gemeinsame Lageerfassung und eine mangelnde gemeinsame Cyber-Krisenreaktion.

Mit der Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie) sollen diese Unterschiede zwischen den nationalen Regelungen der EWR-Mitgliedstaaten beseitigt werden, indem insbesondere

- Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden,
- Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen EWR-Mitgliedstaaten vorgesehen werden,
- die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und
- wirksame Abhilfe- und Durchsetzungsmassnahmen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind,

eingeführt werden.

Die Richtlinie (EU) 2022/2555 enthält rechtliche Massnahmen, um das Cybersicherheitsniveau im EWR insgesamt zu erhöhen, indem Folgendes sichergestellt wird:

- Bereitschaft der EWR-Mitgliedstaaten zur Durchsetzung der Vorgaben der Richtlinie (EU) 2022/2555. Insbesondere wird vorausgesetzt, dass die entsprechenden Behörden in den EWR-Mitgliedstaaten angemessen ausgestattet sind, beispielsweise mit einem sogenannten Computer-Notfallteam (CSIRT).

- Die Zusammenarbeit zwischen allen EWR-Mitgliedstaaten durch Einsetzung einer Kooperationsgruppe zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den EWR-Mitgliedstaaten.
- Das Bestehen einer sektorübergreifenden Sicherheitskultur, die für unsere Wirtschaft und Gesellschaft von entscheidender Bedeutung ist und in hohem Masse auf Informations- und Kommunikationstechnik (IKT) wie Energie, Verkehr, Wasser, Banken, Finanzmarktinfrastrukturen, Gesundheitswesen und digitale Infrastruktur angewiesen ist.

Mit der Durchführung der Verordnung (EU) 2019/881 wird in Liechtenstein die rechtliche Grundlage für Cybersicherheitszertifizierungen im Sinne des europäischen Zertifizierungsrahmens für die Cybersicherheit gemäss der erwähnten Verordnung geschaffen. Der EWR-Rahmen für die Cybersicherheitszertifizierung für IKT-Produkte ermöglicht die Schaffung massgeschneiderter und risikobasierter EWR-Zertifizierungssysteme.

Die Zertifizierung spielt eine zentrale Rolle bei der Steigerung des Vertrauens und der Sicherheit in wichtigen Produkten und Dienstleistungen für die digitale Welt. Der Zertifizierungsrahmen wird EWR-weite Zertifizierungssysteme als umfassendes Regelwerk, technische Anforderungen, Normen und Verfahren bereitstellen. Die daraus resultierenden Zertifikate werden in allen EWR-Mitgliedstaaten anerkannt, was es Unternehmen erleichtern soll, grenzüberschreitend zu handeln und die Sicherheitsmerkmale eines IKT-Produkts oder einer Dienstleistung zu verstehen.

2. BEGRÜNDUNG DER VORLAGE

Die gegenständliche Vorlage betreffend die Totalrevision des Cyber-Sicherheitsgesetzes dient der Umsetzung der Richtlinie (EU) 2022/2555 ins

liechtensteinische Recht. Die Richtlinie (EU) 2022/2555 ist in den EU-Mitgliedstaaten am 16. Januar 2023 in Kraft getreten und ist von den EU-Mitgliedsstaaten bis zum 17. Oktober 2024 umzusetzen.

Für die EWR/EFTA-Staaten gilt das Datum des Inkrafttretens des entsprechenden EWR-Übernahmebeschlusses als Umsetzungsfrist für die Richtlinie (EU) 2022/2555. Mit der gegenständlichen Vorlage kommt Liechtenstein seiner Verpflichtung nach dem EWR-Abkommen nach.

Die Richtlinie (EU) 2022/2555 befindet sich derzeit noch im Übernahmeverfahren ins EWR-Abkommen, wobei das Inkrafttreten des entsprechenden EWR-Übernahmebeschlusses derzeit noch nicht absehbar ist. Jedoch soll die Richtlinie (EU) 2022/2555 möglichst zeitnah ins EWR-Abkommen übernommen werden, um eine einheitliche Rechtslage im gesamten EWR zu schaffen.

Die Verordnung (EU) 2019/881 ist in den EU-Mitgliedstaaten am 27. Juni 2019 in Kraft getreten. Der Gemeinsame EWR-Ausschuss hat die Verordnung (EU) 2019/881 mit Beschluss Nr. 22/2023 bereits ins EWR-Abkommen übernommen. Aufgrund der Tatsache, dass einer der drei EWR/EFTA-Staaten den entsprechenden verfassungsrechtlichen Vorbehalt gemäss Art. 103 des EWR-Abkommens noch nicht aufgehoben hat, ist das Inkrafttreten der Verordnung (EU) 2019/881 jedoch nach wie vor ausstehend.

Die Verordnung (EU) 2019/881 wird mit ihrer Übernahme ins EWR-Abkommen grundsätzlich in Liechtenstein unmittelbar anwendbar. Allerdings enthält die Verordnung (EU) 2019/881 Bestimmungen, die sich unmittelbar an die EWR-Mitgliedstaaten richten und eine Durchführung im nationalen Recht erfordern. Folglich soll die Verordnung (EU) 2019/881 im Zuge der Totalrevision des Cyber-Sicherheitsgesetzes durchgeführt werden.

2.1 Verordnung (EU) 2019/817

Im Rahmen des Gesetzgebungsverfahrens zum CSG im Frühjahr 2023 stellte sich die Frage, ob allenfalls nicht auch die Schengen Verordnung (EU) 2019/817 im Cyber-Sicherheitsgesetz zu berücksichtigen gewesen wäre. Im Zuge der Ausarbeitung dieser Vorlage wurde daher die Gelegenheit genutzt und evaluiert, inwieweit die Stabsstelle Cyber-Sicherheit bei der Durchführung der erwähnten Verordnung (EU) 2019/817 zukünftig unterstützen kann und wo allenfalls zwischen der NIS-2 Richtlinie und der Verordnung Synergien bestehen, die genutzt werden könnten.

Sämtliche betroffenen Stellen, dies sind die Landespolizei, das Amt für Informatik sowie das Ausländer- und Passamt, wurden gehört, um den Status quo der Durchführung der Verordnung (EU) 2019/817, die Zeitplanung, die geplanten organisatorischen Strukturen sowie die technischen Möglichkeiten zu bewerten. Mögliche Synergien bei der Umsetzung bzw. Durchführung der erwähnten EU-Rechtsakten sollten identifiziert werden, um in weiterer Folge, durch die entsprechende Ausgestaltung der Organisation (innerhalb der LLV), den Aufwand und den Ressourcenbedarf bei den einzelnen Stellen und Ämtern, möglichst gering zu halten. Der Aufbau von doppelten Strukturen soll vermieden werden.

Im Ergebnis wurde festgestellt, dass bei der aktuellen Totalrevision des CSG vorerst nichts Konkretes berücksichtigt werde muss. Es wurde festgestellt, dass die Verordnung (EU) 2019/817 nicht EWR-relevant ist, sondern es sich um eine Weiterentwicklung des Schengen-Besitzstandes handelt.

Die Hauptzuständigkeiten in Bezug auf die Informationssysteme der EU, sprich das Einreise-/Ausreisesystem («EES»), das Visa-Informationssystem («VIS»), das Europäische Reiseinformations- und Reisegenehmigungssystem («ETIAS»), Eurodac, das Schengener Informationssystem («SIS») und das Europäische

Strafregisterinformationssystem für Drittstaatsangehörige («ECRIS-TCN»), liegen bei der Landespolizei und beim Ausländer- und Passamt. Dort sind diese auch richtig verortet.

3. SCHWERPUNKTE DER VORLAGE

Zur Umsetzung der Richtlinie (EU) 2022/2555 und der Durchführung der Verordnung (EU) 2019/881 wird die Totalrevision des Cyber-Sicherheitsgesetzes (CSG) vorgeschlagen.

Die gegenständliche Vernehmlassungsvorlage orientiert sich hinsichtlich des Aufbaus und der Wortwahl an der umzusetzenden Richtlinie (EU) 2022/2555. Die Gliederung der Vorlage entspricht dem aktuellen Cyber-Sicherheitsgesetz.

Die Vernehmlassungsvorlage enthält in Kapitel I. zunächst allgemeine Bestimmungen, wie beispielsweise den Geltungsbereich, Begriffsbestimmungen und Bezeichnungen.

Im Kapitel II. finden sich die Regelungen betreffend die Risikomanagement- und Sicherheitsmassnahmen sowie der Berichtspflichten.

Kapitel III. enthält die Bestimmungen in Bezug auf Organisation und Durchführung des Gesetzes. Es werden einleitend die Zuständigkeiten bestimmt. Das Kapitel enthält weiters Aufgaben und Befugnisse, inklusive der Kontrollbefugnisse der Stabsstelle Cyber-Sicherheit gegenüber wesentlichen und wichtigen Einrichtungen. Ebenso finden sich in diesem Kapitel Bestimmungen betreffend die Verarbeitung und Offenlegung personenbezogener Daten sowie den Betrieb von Informations- und Kommunikationstechnik-Lösungen (IKT-Lösungen) durch die Stabsstelle Cyber-Sicherheit. Das Kapitel schliesst ab mit Bestimmungen zum sogenannten Computer-Notfallteam (CSIRT) sowie zur nationalen Cybersicherheitsstrategie.

In Kapitel IV ist die Beschwerdemöglichkeit geregelt.

Kapitel V enthält Bestimmungen zu den Verwaltungsübertretungen (Strafbestimmungen) sowie zu den Verantwortlichkeiten.

Abschliessend enthält die Vernehmlassungsvorlage in Kapitel IV. noch die Schlussbestimmungen, wie beispielsweise eine Verordnungskompetenz, die Aufhebung des bisherigen Cyber-Sicherheitsgesetzes und das Inkrafttreten.

4. ERLÄUTERUNGEN ZU DEN EINZELNEN ARTIKELN

Zu Art. 1 – Gegenstand und Geltungsbereich

In Art. 1 werden der Gegenstand und der Geltungsbereich des Gesetzes festgelegt. Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Die Sicherstellung ihrer Verlässlichkeit und Sicherheit ist deshalb von grosser Bedeutung und mit entsprechenden Massnahmen soll ein hohes, dem Risiko angemessenes Cybersicherheitsniveau erreicht werden.

Der Anwendungsbereich dieses Gesetz umfasst gemäss **Abs. 1** öffentliche und private Einrichtungen der im Anhang 1 und 2 genannten Art, die als mittelgrosse oder grosse Gesellschaften gelten und ihre Dienste im EWR erbringen oder ihre Tätigkeiten dort ausüben. Der Anwendungsbereich ergibt sich somit vor allem aufgrund der Grösse, sprich der Anzahl Arbeitnehmerinnen und Arbeitnehmer sowie des Jahresumsatzes oder der Jahresbilanz, sofern sie als eine in Anhang 1 oder 2 genannte Art einer Einrichtung zu qualifizieren sind.

Was unter grossen und mittelgrossen Gesellschaften bzw. Einrichtungen zu verstehen ist, wird in Art. 1064 Personen- und Gesellschaftsrecht (PGR) geregelt. So sind grosse Gesellschaften Einrichtungen, die zumindest zwei der drei folgenden Merkmale überschreiten: 1. 25.9 Millionen Schweizer Franken

Bilanzsumme; 2. 51.8 Millionen Schweizer Franken Nettoumsatzerlöse im dem Bilanzstichtag vorangehenden Geschäftsjahr und 3. im Durchschnitt des Geschäftsjahres 250 Arbeitnehmerinnen und Arbeitnehmer beschäftigen.

Als mittelgrosse Gesellschaften bzw. Einrichtungen gelten, wenn sie mindestens zwei der folgenden Merkmale überschreiten und mindestens zwei der drei zuvor erwähnten Merkmale für grosse Gesellschaften nicht überschreiten: 1. 7.4 Millionen Schweizer Franken Bilanzsumme; 2. 14.8 Millionen Schweizer Franken Nettoumsatzerlöse im dem Bilanzstichtag vorangehenden Geschäftsjahr und 3. im Durchschnitt des Geschäftsjahres 50 Arbeitnehmerinnen und Arbeitnehmer beschäftigen.

Bei der Prüfung des Anwendungsbereichs im Zusammenhang mit der Unternehmensgrösse ist die Kerntätigkeit des Unternehmens von zentraler Bedeutung. So kann alleine aufgrund des Umstands, dass eine grosse oder mittelgrosse Einrichtung etwa ein Rechenzentrum (vgl. Anhang 1 Ziff. 8, Anbieter von Rechenzentrumsdiensten) oder Ladestationen für Fahrzeuge auf dem Firmengelände betreibt (vgl. Anhang 1 Ziff. 1, Betreiber von Ladepunkten) nicht zwingend davon ausgegangen werden, dass das Cyber-Sicherheitsgesetz für diese Einrichtung zur Anwendung kommt. Vielmehr kommt es auf die Haupttätigkeit der Einrichtung im Sinne des Geschäftszwecks an, was in Abgrenzung zu einer allfälligen Nebentätigkeit zu sehen ist.

Daneben gilt unabhängig von der Grösse der Einrichtungen das Gesetz gemäss **Abs. 2** ebenso für Einrichtungen der im Anhang 1 und 2 genannten Art, sofern die jeweilige Einrichtung in den Bst. a bis f Erwähnung findet.

Gemäss **Bst a. Ziff. 1** gilt das Gesetz ebenso für Anbieter von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten. Öffentliche elektronische

Kommunikationsnetze sind gemäss Art. 3 Abs. 1 Ziff. 13 und 15 KomG legaldefiniert. Es handelt sich dabei um Übertragungssysteme und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitige Ressourcen – einschliesslich der nicht aktiven Netzbestandteile –, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Einrichtungen ermöglichen, einschliesslich Satellitennetze, feste (leitungs- und paketvermittelte, einschliesslich Internet) und mobile terrestrische Netze, Stromleitungssysteme, soweit sie zur Signalübertragung genutzt werden, Netze für Hör- und Fernsehfunk sowie Kabelfernsehnetze, die ganz oder überwiegend der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste dienen. Ein öffentlich zugänglicher Kommunikationsdienst ist gemäss Art. 3 Abs. 1 Ziff. 10 KomG ein elektronischer Kommunikationsdienst, der einer breiten Öffentlichkeit zur Verfügung steht, einschliesslich eines öffentlich zugänglichen Telefondienstes. Wegen ihrer Bedeutung für die Aufrechterhaltung der Funktionsfähigkeit öffentlicher Informations- und Kommunikationstechnologie fallen Einrichtungen bzw. Betreiber, die derartige öffentliche Dienste anbieten, schon heute in den Anwendungsbereich des CSG bzw. der Cyber-Sicherheitsverordnung (CSV) gemäss Art. 10 Bst. d und e CSV. Mit der Umsetzung der Richtlinie (EU) 2022/2555 werden jene Bestimmungen der Richtlinie (EU) 2018/1972, mit denen diesen Einrichtungen bzw. Betreibern Sicherheitsanforderungen und Berichtspflichten auferlegt werden (national umgesetzt mit Kommunikationsgesetz, LGBl. 2023 Nr. 216), nun gestrichen. Die Vorschriften über die Berichtspflichten gemäss dem vorliegenden Gesetz lassen die Vorschriften der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG unberührt.

Gemäss **Bst. a Ziff. 2 und 3** gilt das Gesetz unabhängig der Grösse auch für Vertrauensdiensteanbieter gemäss Art. 3 Abs. 1 Ziff. 26, TLD-Namenregistern gemäss Art. 3 Abs. 1 Ziff. 21 und DNS-Diensteanbietern gemäss Art. 3 Abs. 1 Ziff.

22. Dieses Gesetz gilt nicht für Root-Namenserver. Mit der Aufnahme von Vertrauensdiensteanbieter i.S.d. Verordnung (EU) Nr. 910/2014 in den Anwendungsbereich dieses Gesetzes, soll sichergestellt werden, dass auch für diese Gruppe ein hohes Niveau an Sicherheitsanforderungen und der Aufsicht gewährleistet wird. Vom Anwendungsbereich ausgenommen bleibt weiterhin die Erbringung von Vertrauensdiensten, die ausschliesslich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden. Die im vorliegenden Gesetzesentwurf festgelegten Cybersicherheitspflichten dienen dabei als Ergänzung zu den Anforderungen, denen Vertrauensdiensteanbieter gemäss der Verordnung (EU) Nr. 910/2014 heute unterliegen.

Vertrauensdiensteanbieter werden nun verpflichtet, alle geeigneten und verhältnismässigen Massnahmen zu ergreifen, um die sich für ihre Dienste, aber auch ihre Kunden und vertrauende Dritte ergebenden Risiken zu beherrschen und Sicherheitsvorfälle gemäss diesem Gesetzesentwurf zu melden. Diese Cybersicherheits- und Berichtspflichten betreffen auch den physischen Schutz der angebotenen Dienste. Die Anforderungen an qualifizierte Vertrauensdiensteanbieter gemäss Art. 24 der Verordnung (EU) Nr. 910/2014 gilt weiterhin. Die entsprechenden Bestimmungen der Verordnung (EU) Nr. 910/2014, mit denen diesen Arten von Einrichtungen Sicherheitsanforderungen und Berichtspflichten auferlegt werden, werden daher gestrichen. Die Vorschriften über die Berichtspflichten gemäss dem vorliegenden Gesetz lassen die Vorschriften der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG unberührt.

Das Gesetz gilt ungeachtet der Grösse gemäss **Bst. b** ebenso für Einrichtungen, wenn es sich bei der Einrichtung um den einzigen Anbieter handelt, der einen Dienst erbringt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder

wirtschaftlicher Tätigkeiten unerlässlich ist. Mit dieser Bestimmung wird Art. 2 Abs. 2 Bst. b der Richtlinie (EU) 2022/2555 umgesetzt und ist gerade für Liechtenstein von zentraler Bedeutung. Dies vor allem, weil nicht zuletzt Unternehmen und Einrichtungen mit wenigen Mitarbeitenden wichtige und kritische Dienste im Land betreiben oder erbringen.

Ebenso gilt das Gesetz für Einrichtungen, wenn sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte (**Bst. c**), 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 (**Bsd. d**) oder 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 EWR-Mitgliedstaat hat, kritisch ist (**Bst. e**). Gemäss Bst. c wird der Anwendungsbereich beispielsweise auf das Notrufsystem und in weiterer Folge auf die Landesnotruf- und Einsatzzentrale der Landespolizei (LNEZ) bei der Landespolizei ausgedehnt.

Ebenso gilt dieses Gesetz gemäss **Bst. f** für Einrichtungen der öffentlichen Verwaltung. Damit findet die gegenständliche Vorlage vollumfänglich Anwendung auf die Liechtensteinische Landesverwaltung und deren Ämter und Stabsstellen.

Abs. 3 legt weiter fest, dass dieses Gesetz ebenso unabhängig der Grösse für Einrichtungen gilt, die als kritische Einrichtung gemäss Richtlinie (EU) 2022/2557 eingestuft wurden (**Bst. a**) oder einen Domänennamenregistrierungsdienst gemäss Art. 3 Abs. 1 Ziff. 23 (**Bst. b**) erbringen. Kritische Einrichtungen gemäss Richtlinie (EU) 2022/2557 sind öffentliche oder private Einrichtungen, die einen oder mehrere wesentliche Dienste in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale

Infrastruktur, öffentliche Verwaltung, Weltraum sowie der Produktion, Verarbeitung und Vertrieb von Lebensmitteln erbringen und in Liechtenstein tätig sind, die ihre kritische Infrastruktur – Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind – in Liechtenstein betreiben.

Abs. 4 bestimmt schliesslich, für welche Einrichtungen im Falle der Anwendbarkeit dieser Vorlage die darin vorgesehenen Risikomanagementmassnahmen und Berichtspflichten gemäss Art. 4 und 6 nicht gelten sollen. Dies sind gemäss **Bst. a** 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. Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten nur geringfügig mit diesen Bereichen zusammenhängen, sind jedoch nicht von den Risikomanagementmassnahmen und Berichtspflichten ausgenommen. Ebenso gilt diese Ausnahme in Bezug auf die Risikomanagementmassnahmen und Berichtspflichten nicht für die Landesnotruf- und Einsatzzentrale der Landespolizei (LNEZ). Dies insbesondere, weil die Landespolizei den landesweiten Sanitätsnotruf 144 betreut, indem sie die Sanitätsnotrufe entgegennimmt, die gemeldeten Notfallsituationen einer ersten Beurteilung unterzieht und den dafür geeigneten Rettungsdienst aufbietet.

Weiters gelten die Risikomanagementmassnahmen und Berichtspflichten gemäss Art. 4 und 6 nicht für Einrichtungen, die gemäss Art. 2 Abs. 4 der Verordnung (EU) 2022/2554[1] vom Anwendungsbereich dieser Verordnung ausgenommen sind

[1] Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (Abl. L 333 vom 27.12.2022, S. 1-79)

(**Bst. b**). In diesem Zusammenhang wird auf die Durchführung der Verordnung (EU) 2022/2554 verwiesen. Hier hat die Finanzmarktaufsicht (FMA) die Federführung.

Zu Art. 2 – Umsetzung und Durchführung von EWR-Rechtsvorschriften

In **Abs. 1** werden jene EWR-Rechtsvorschriften aufgezählt, welche mit der gegenständlichen Vorlage umgesetzt bzw. durchgeführt werden. Dies sind die Richtlinie (EU) 2022/2555 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie) (**Bst. a**), die Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (**Bst. b**) und Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (**Bst. c**).

Seit dem 1. Februar 2021 erfolgt die Kundmachung des verbindlichen Wortlauts von EWR-Rechtsvorschriften durch eine vereinfachte Publikation und einen direkten Verweis auf das Amtsblatt der Europäischen Union (ABl.). Die Bezugnahme auf die genannten EU-Rechtsakte erfolgt deshalb neu in verkürzter Form. Der Volltitel der Richtlinie sowie deren Fundstelle im ABl. finden sich in der entsprechenden Fussnote.

Die gültige Fassung der EWR-Rechtsvorschriften, auf die in diesem Gesetz Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes (**Abs. 2**).

Zu Art. 3 – Begriffsbestimmungen und Bezeichnungen

In **Abs. 1** finden sich die Begriffsbestimmungen. Wo es keiner für Liechtenstein spezifischen Legaldefinition bedarf oder nicht anderweitig aufgeführt, wurden die in Art. 6 der Richtlinie (EU) 2022/2555 geregelten Definitionen wortgleich in die Vorlage übernommen.

«Netz- und Informationssysteme» (**Ziff. 1**) sind elektronische Kommunikationsnetze, wie sie auch in Art. 3 Abs. 1 Ziff. 13 des Gesetzes über die elektronische Kommunikation (Kommunikationsgesetz; KomG) definiert werden. Darüber hinaus versteht man darunter auch räumlich verteilte, digitale Verarbeitungsvorrichtungen zur technischen Unterstützung der Erhebung, Verarbeitung, Speicherung, Wartung, Nutzung, Weitergabe, Verbreitung oder Disposition von Informationen. Auch die Daten, die in einem solchen elektronischen Kommunikationsnetz oder einer solchen Vorrichtung verarbeitet werden, sind von dem Begriff umfasst. Die Begriffsdefinition wurde aus der Richtlinie (EU) 2022/2555 übernommen und entspricht auch der Bestimmung im Art. 3 Abs. 1 Bst. a CSG, wobei lediglich der Begriff «Gerät» in Bst. b den bisherigen Begriff «Vorrichtung» ersetzt.

«Sicherheit von Netz- und Informationssystemen» (**Ziff. 2**) ist 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. Sie umfasst nicht nur die Fähigkeit, Sicherheitsvorfälle abzuwehren, sondern auch die Fähigkeit, Sicherheitsvorfällen präventiv vorzubeugen, eine bereits entstandene Störung zu erkennen, zu beseitigen und möglichst rasch den Normalbetrieb wiederherzustellen.

«Cybersicherheit» (**Ziff. 3**) bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen.

«NIS-Strategie» (Nationale Cybersicherheitsstrategie) (**Ziff. 4**) ist ein kohärenter Rahmen mit strategischen Zielen und Prioritäten im Bereich der Cybersicherheit und der zu ihrer Verwirklichung erforderlichen Governance. Der Grundsatz und weitere Regelungen betreffend die NIS-Strategie finden sich in Art. 19.

Ein «Beinahe-Vorfall» (**Ziff. 5**) beschreibt jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde oder das nicht eingetreten ist.

Von einem «Sicherheitsvorfall» (**Ziff. 6**) wird gesprochen, wenn ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt. Die Begriffsdefinition wurde aus der Richtlinie (EU) 2022/2555 übernommen und entspricht im Wortlaut Art. 3 Abs. 1 Bst. i CSG.

Ein Sicherheitsvorfall ist gemäss **Ziff. 7** erheblich, wenn er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann (**Bst. a**) oder andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann (**Bst. b**). Die Begriffsdefinition wurde aus Art. 23 Abs. 3 der Richtlinie (EU) 2022/2555 entsprechend übernommen.

Ein «Cybersicherheitsvorfall grossen Ausmasses» (**Ziff. 8**) ist ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmass die Reaktionsfähigkeit eines EWR-

Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei EWR-Mitgliedstaaten hat.

Die «Bewältigung von Sicherheitsvorfällen» (**Ziff. 9**) umfasst alle Massnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon.

Ein «Risiko» nach **Ziff. 10** ist 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.

Eine «Cyberbedrohung» (**Ziff. 11**) ist ein möglicher Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte.

Eine Cyberbedrohung ist gemäss **Ziff. 12** erheblich, wenn sie 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.

Ein «IKT-Produkt» (**Ziff. 13**) ist ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems. Ein «IKT-Dienst» (**Ziff. 14**) ist ein Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht und ein «IKT-Prozess» (**Ziff. 15**) beschreibt jegliche Tätigkeit, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.

Eine «Schwachstelle» (**Ziff. 16**) ist jede Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann.

Eine «Norm» gemäss **Ziff. 17** ist eine Norm im Sinne des Art. 2 Ziff. 1 der Verordnung (EU) Nr. 1025/2012. Eine «technische Spezifikation» (**Ziff. 18**) ist eine technische Spezifikation im Sinne des Art. 2 Ziff. 4 der Verordnung (EU) Nr. 1025/2012.

Ein «Internet-Knoten» gemäss **Ziff. 19** ist 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.

Das «Domänennamensystem (DNS)» (**Ziff. 20**) ist 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.

Ein «DNS-Diensteanbieter» nach **Ziff. 21** ist eine Einrichtung, die für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domänennamen anbietet (**Bst. a**) oder autoritative Dienste zur Auflösung von Domänennamen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet (**Bst. b**). Personen, die DNS-Auflösungsdienste für Familienangehörige anbieten, sind nicht als DNS-Diensteanbieter zu qualifizieren. Es fehlt am Erfordernis der Öffentlichkeit.

In jenen Fällen, in denen DNS ausschliesslich als Teil des Internetzugangsdienstes durch einen Internetserviceprovider (ISP) bereitgestellt wird, wird der DNS als Teil des Internetzugangsdienstes angesehen und in diesem Fall nicht als eigenständiger Dienst behandelt. Dies bedeutet, dass für einen ISP, der DNS-Auflösungsdienste ausschliesslich als Teil des Internetzugangsdienstes anbietet, die Bestimmung nach Art. 1 Abs. 2 Bst. a Ziff. 3 dieses Gesetztes, sprich die Anwendbarkeit ungeachtet der Grösse der Einrichtung, nicht zur Anwendung kommt.

Das «Namenregister der Domäne der ersten Ebene» oder «TLD-Namenregister» (**Ziff. 22**) ist eine Einrichtung, der eine bestimmte Domäne der ersten Ebene (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.

Eine «Einrichtung, die Domänennamen-Registrierungsdienste erbringt» (**Ziff. 23**) ist ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten.

Die Risikomanagementmassnahmen im Bereich der Cybersicherheit und Berichtspflichten gelten nur für wesentliche und wichtige Einrichtungen. Da die Einrichtungen, die Domänennamen registrieren, nicht zur Kategorie der wesentlichen oder wichtigen Einrichtungen gehören, gelten die einschlägigen Bestimmungen über das Risikomanagement im Bereich der Cybersicherheit (Art.

4) und der Berichtspflichten (Art. 6) nicht für diese Einrichtungen. Einrichtungen, die Domänennamen-Registrierungsdienste anbieten unterliegen ungeachtet dessen gemäss Art. 1 Abs. 3 Bst. b den Bestimmungen dieses Gesetzes und die Stabsstelle Cyber-Sicherheit hat gemäss Art. 13 Abs. 1 Bst. e auch die Aufgabe, eine Liste von Einrichtungen zu erstellen, die Domänennamen-Registrierungsdienste erbringen.

Ein «digitaler Dienst» nach **Ziff. 24** ist ein Dienst im Sinne des Art. 1 Abs. 1 Bst. b der Richtlinie (EU) 2015/1535.

Ein «Vertrauensdienst» (**Ziff. 25**) ist ein Vertrauensdienst im Sinne des Art. 3 Ziff. 16 der Verordnung (EU) Nr. 910/2014 (nachfolgend eIDAS-VO), ein «Vertrauensdiensteanbieter» (**Ziff. 26**) ein Vertrauensdiensteanbieter im Sinne des Art. 3 Ziff. 19 eIDAS-VO, ein «qualifizierter Vertrauensdienst» (**Ziff. 27**) ein qualifizierter Vertrauensdienst im Sinne des Art. 3 Ziff. 17 eIDAS-VO und ein «qualifizierter Vertrauensdiensteanbieter» (**Ziff. 28**) ein qualifizierter Vertrauensdiensteanbieter im Sinne des Art. 3 Ziff. 20 eIDAS-VO.

Die eIDAS-VO wurde im Gesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz; SigVG) durchgeführt und es wurden keine von der genannten Verordnung abweichenden Definitionen festgelegt. Art. 2 Abs. 1 Bst. a SigVG verweist für den «VDA», den Vertrauensdiensteanbieter, bei der Begriffsbestimmung ebenfalls auf Art. 3 Ziff. 19 eIDAS-VO.

Ein «Online-Marktplatz» (**Ziff. 29**) ermöglicht es Verbrauchern und Unternehmern, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschliessen, und ist der endgültige Bestimmungsort für den Abschluss dieser Verträge. Der Begriff des «Online-Marktplatzes» erstreckt sich nicht auf Online-Dienste, die lediglich als Vermittler für Drittdienste fungieren, durch die letztlich

ein Vertrag geschlossen werden kann. Online-Dienste, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschliessend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft, sind daher nicht erfasst. Die von dem Online-Marktplatz bereitgestellten IT-Dienste können die Verarbeitung von Transaktionen, die Aggregation von Daten oder die Erstellung von Nutzerprofilen einschliessen.

Eine «Online-Suchmaschine» (**Ziff. 30**) ermöglicht es dem Nutzer, Suchen grundsätzlich auf allen Internetseiten anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Sie kann alternativ dazu auf Internetseiten in einer bestimmten Sprache beschränkt sein. Die Definition des Begriffs «Online-Suchmaschine» in diesem Gesetz erstreckt sich nicht auf Suchfunktionen, die auf den Inhalt einer bestimmten Internetseite beschränkt sind, unabhängig davon, ob diese Suchfunktionen durch eine externe Suchmaschine bereitgestellt werden. Sie erstreckt sich auch nicht auf Online-Dienste, die die Preise für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern miteinander vergleichen und den Nutzer anschliessend an den bevorzugten Unternehmer weiterleiten, damit er das Produkt dort kauft.

«Cloud-Computing-Dienste» nach **Ziff. 31** sollten digitale Dienste umfassen, die auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind. Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service). Die Bereitstellungsmodelle für Cloud- Computing sollten die private, die

gemeinschaftliche, die öffentliche und die hybride Cloud umfassen. Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden.

Der Begriff «umfassender Fernzugang» wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschliesslich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern. Der Begriff «skalierbar» bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff «elastischer Pool» wird verwendet, um Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann. Der Begriff «gemeinsam nutzbar» wird verwendet, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird. Der Begriff «verteilt» wird verwendet, um Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.

Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil

einer Cloud-Computing-Infrastruktur. Um allen Risiken für die Sicherheit von Netz- und Informationssystemen zu begegnen, sind auch jene Anbieter von Rechenzentrumsdiensten vom Anwendungsbereich dieses Gesetzes erfasst, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Der Begriff «Rechenzentrumsdienst» nach **Ziff. 32** umfasst Dienste, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie (IT) und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff «Rechenzentrumsdienst» gilt nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden.

Ein «Inhaltszustellnetz» (Englisch «content delivery network»; CDN) (**Ziff. 33**) 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. Digitale Inhalte sind alle Arten von digitalen Daten, sowohl statische als auch sich dynamisch verändernde Daten.

Eine «Plattform für Dienste sozialer Netzwerke» (**Ziff. 34**) ist 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.

Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Anbietern von

verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Anbietern von Online-Suchmaschinen sowie Anbieter von Plattformen für Dienste sozialer Netzwerke grenzübergreifenden Charakter haben, ist jeweils immer nur ein EWR-Mitgliedstaat für diese Einrichtungen zuständig. Die Zuständigkeit liegt bei dem EWR-Mitgliedstaat, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat.

Ein «Vertreter» gemäss **Ziff. 35** ist eine im EWR 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 im EWR 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 dieses Gesetzes wenden kann.

Ein «öffentliches elektronisches Kommunikationsnetz» nach **Ziff. 36** ist ein öffentliches elektronisches Kommunikationsnetz im Sinne von Art. 3 Abs. 1 Ziff. 15 KomG und ein «elektronischer Kommunikationsdienst» nach **Ziff. 37** ist ein elektronischer Kommunikationsdienst im Sinne des Art. 3 Abs. 1 Ziff. 8 KomG.

Eine «Einrichtung» nach **Ziff. 38** kann sowohl eine natürliche Person als auch nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person sein, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann. Die Definition entspricht jener in Art. 6 Ziff. 38 der Richtlinie (EU) 2022/2555.

Ein «Anbieter verwalteter Dienste» **(Ziff. 39)** ist 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. Von dieser Begriffsdefinition sind auch Einrichtungen umfasst, die Kundennetze warten und betreuen, sprich klassische IT-Dienstleister. Dabei spielt es keine Rolle, ob die Dienstleistung vor Ort oder aus der Ferne erbracht wird.

Ein «Anbieter verwalteter Sicherheitsdienste» (**Ziff. 40**) ist ein Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt. Beispiele für Sicherheitsdienstleistungen die ein Anbieter erbringt finden sich in Art. 5 Abs. 2, wie etwa die Erstellung und Umsetzung von Konzepten in Bezug auf die Risikoanalyse und Sicherheit der Informationssysteme, die Unterstützung bei der Bewältigung von Sicherheitsvorfällen sowie die Implementierung einer Backup-Lösung. Die gegenständliche Begriffsdefinition basiert auf der Definition des Begriffs Anbieter verwalteter Dienste (Ziff. 39), der sich auf die Installation, die Verwaltung, den Betrieb oder die Wartung von IKT-Produkten, -Netzen, -Infrastrukturen, -Anwendungen oder anderen Netzen bezieht und daher eine gewisse aktive technische Unterstützung erfordert. Reine Beratungsdienste erfüllen daher die Anforderungen der Ziff. 40 nicht.

Forschungstätigkeiten spielen eine Schlüsselrolle bei der Entwicklung neuer Produkte und Prozesse. Viele dieser Tätigkeiten werden von Einrichtungen durchgeführt, die ihre Forschungsergebnisse zu kommerziellen Zwecken teilen, verbreiten oder nutzen. Diese Einrichtungen können daher wichtige Akteure in Wertschöpfungsketten sein. Unter «Forschungseinrichtungen» **(Ziff. 41)** sind

unter anderem Einrichtungen zu verstehen, die sich im Wesentlichen auf die Durchführung von angewandter Forschung oder experimenteller Entwicklung im Sinne des Frascati-Handbuchs der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung von 2015 (Leitlinien zur Erfassung von Daten zu Forschung und experimenteller Entwicklung sowie zur entsprechenden Berichterstattung) konzentrieren, um ihre Ergebnisse für kommerzielle Zwecke wie die Herstellung oder Entwicklung eines Produkts oder eines Verfahrens, die Erbringung eines Dienstes, oder dessen Vermarktung zu nutzen. Bildungseinrichtungen sind jedoch von dieser Begriffsdefinition ausgeschlossen.

Die Kooperationsgruppe, das CSIRTs-Netzwerk und EU-CyCLONe sind verschiedenste EU/EWR-Gremien. Die «Kooperationsgruppe» (**Ziff. 42**) ist ein nach Art. 14 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der EWR-Mitgliedstaaten, der Europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zusammensetzt und der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den EWR-Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen Cybersicherheitsniveaus im EWR dient. Die Kooperationsgruppe wurde mit der Richtlinie (EU) 2016/1148 eingeführt und die Stabsstelle Cyber-Sicherheit nimmt seit November 2022 regelmässig an diesen Sitzungen teil. Es finden bis zu vier Sitzungen im Jahr statt.

Das «CSIRTs-Netzwerk» (**Ziff. 43**) ist ein nach Art. 15 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der Computer-Notfallteams der EWR-Mitgliedstaaten und des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) zusammensetzt und zum Aufbau von Vertrauen zwischen den EWR-Mitgliedstaaten beitragen sowie eine rasche und wirksame operative Zusammenarbeit fördern soll. Das CSIRTs-Netzwerk wurde

ebenfalls mit der Richtlinie (EU) 2016/1148 eingeführt und erhält mit der Richtlinie (EU) 2022/2555 zusätzliche Aufgaben.

«EU-CyCLONe» (European Cyber Crises Liaison Organisation Network) (**Ziff. 44**) ist ein nach Art. 16 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der Behörden für das Cyberkrisenmanagement der EWR-Mitgliedstaaten und der Europäischen Kommission zusammensetzt und bei der koordinierten Bewältigung von Cybersicherheitsvorfällen grossen Ausmasses und Krisen auf operativer Ebene sowie bei der Gewährleistung eines regelmässigen Austauschs relevanter Informationen zwischen den EWR-Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen unterstützen soll. EU-CyCLONe ist somit ein Kooperationsnetzwerk für die nationalen Behörden der Mitgliedstaaten, die für das Cyberkrisenmanagement zuständig sind.

Wesentliche Aufgaben von EU-CyCLONe sind die Unterstützung der koordinierten Bewältigung gross angelegter Cybersicherheitsvorfälle und -krisen auf operativer Ebene und Gewährleistung des regelmässigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen, Ämtern und Agenturen der Union, das Erhöhen des Grads der Vorbereitung bei der Bewältigung gross angelegter Cybersicherheitsvorfälle und -krisen, die Entwicklung eines gemeinsamen Situationsbewusstseins für gross angelegte Cybersicherheitsvorfälle und -krisen, das bewerten der Folgen und Auswirkungen relevanter gross angelegter Cybersicherheitsvorfälle und -krisen, die Koordinierung der Bewältigung gross angelegter Cybersicherheitsvorfälle und -krisen sowie die Unterstützung der Entscheidungsfindung auf politischer Ebene in Bezug auf solche Vorfälle und Krisen.

Bei Einrichtungen, die für die Zwecke der Einhaltung von Risikomanagementmassnahmen und der Berichtspflichten im Bereich der Cybersicherheit in den Geltungsbereich dieses Gesetzes fallen, werden zwei

Kategorien unterschieden: Erstens sind dies die wesentlichen Einrichtungen (**Abs. 2**) und zweitens die wichtigen Einrichtungen (**Abs. 3**) . Berücksichtigt werden dabei der Grad ihrer Kritikalität in Bezug auf ihren Sektor oder die Art der von ihnen erbrachten Dienste sowie ihre Grösse. Bei den Aufsichts- und Durchsetzungsregelungen wird zwischen diesen beiden Kategorien von Einrichtungen differenziert, um ein ausgewogenes Verhältnis zwischen risikobasierten Anforderungen und Pflichten einerseits und dem Verwaltungsaufwand, der sich andererseits aus der Überwachung der Einhaltung ergibt, zu gewährleisten.

Wesentliche Einrichtungen werden in **Abs. 2** definiert. Darunter fallen nach **Bst. a** alle Einrichtungen der in Anhang 1 aufgeführten Art, die die in Art. 1064 Abs. 2 PGR genannten Schwellenwerte für mittelgrosse Gesellschaften überschreiten, sprich es sich um grosse Gesellschaften im Sinne des PGR handelt. Grosse Gesellschaften sind Einrichtungen, die zumindest zwei der drei folgenden Merkmale überschreiten: 1. 25.9 Millionen Schweizer Franken Bilanzsumme; 2. 51.8 Millionen Schweizer Franken Nettoumsatzerlöse im dem Bilanzstichtag vorangehenden Geschäftsjahr und 3. im Durchschnitt des Geschäftsjahres 250 Arbeitnehmerinnen und Arbeitnehmer beschäftigen.

Um zu vermeiden, dass Einrichtungen, die Partnerunternehmen haben oder verbundene Unternehmen sind, als wesentliche oder wichtige Einrichtungen betrachtet werden, wenn dies unverhältnismässig wäre, ist der Grad der Unabhängigkeit einer Einrichtung gegenüber ihren Partnerunternehmen und verbundenen Unternehmen bei der Beurteilung durch die Stabsstelle Cyber-Sicherheit zu berücksichtigen. Insbesondere in jenen Fällen, in denen eine Einrichtung in Bezug auf die Netz- und Informationssysteme, die sie bei der Erbringung ihrer Dienste nutzt, und in Bezug auf die von ihr erbrachten Dienste unabhängig von ihren Partnerunternehmen oder verbundenen Unternehmen ist.

Bei der Beurteilung orientiert sich die Stabsstelle Cyber-Sicherheit an der Empfehlung 2003/361/EG[2].

Zu den wesentlichen Einrichtungen zählen ebenfalls qualifizierte Vertrauensdiensteanbieter und TLD-Namenregister sowie DNS-Diensteanbieter, unabhängig von ihrer Grösse (**Bst. b**). Es fallen sämtliche Einrichtungen, die öffentlich zugängliches rekursives DNS für Internet-Endnutzer oder autoritatives DNS für Dritte anbieten, unabhängig von ihrer Grösse in den Anwendungsbereich dieses Gesetzes und sind als wesentliche Einrichtung zu qualifizieren. Ein Internet-Diensteanbieter (ISP) wird grundsätzlich bei der Bereitstellung des Internetzugangsdienstes (IAS) ebenso DNS zur Verfügung stellen. Dieser DNS kann als Teil des IAS angesehen werden, da ohne diesen Service die Internetverbindung für den durchschnittlichen Endnutzer praktisch unbrauchbar ist. Folglich werden die DNS-Resolver als Teil des IAS betrachtet und nicht als eigener Dienst. ISPs sind daher aufgrund des Umstands einen DNS zu betreiben nicht zugleich als wesentliche Einrichtung zu qualifizieren.

Zudem zählen zu den wesentlichen Einrichtungen Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Art. 1064 Abs. 2 PGR als mittelgrosse Gesellschaften gelten (**Bst. c**). Als mittelgrosse Gesellschaften gelten, wenn sie mindestens zwei der folgenden Merkmale überschreiten und nicht grosse Gesellschaften sind: 1. 7.4 Millionen Schweizer Franken Bilanzsumme; 2. 14.8 Millionen Schweizer Franken Nettoumsatzerlöse im dem Bilanzstichtag vorangehenden Geschäftsjahr und 3. im Durchschnitt des Geschäftsjahres 50 Arbeitnehmerinnen und Arbeitnehmer beschäftigen.

---

[2] Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (bekannt gegeben unter Aktenzeichen K(2003) 1422) (ABl. L 124 vom 20.5.2003, S. 36-41)

Einrichtungen der öffentlichen Verwaltung sind ebenfalls als wesentliche Einrichtungen zu qualifizieren (**Bst. d**).

Ebenso kann die Regierung mittels Verordnung sonstige Einrichtungen der in Anhang 1 oder 2 aufgeführten Art als wesentliche Einrichtungen einstufen (**Bst. e**). Eine Einstufung durch die Regierung kann jedoch nur in bestimmten abschliessenden Fällen erfolgen. So etwa, wenn es sich bei der Einrichtung um den einzigen Anbieter handelt, der einen bestimmten Dienst erbringt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist oder sich eine Störung des von der betreffenden Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte. Ebenso wäre eine Einstufung durch die Regierung möglich, sofern 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 oder die betreffende 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 EWR-Mitgliedstaat hat, kritisch ist. Der Einstufung der Regierung sind somit Schranken gesetzt.

Schliesslich sind Einrichtungen, die gemäss der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden, nach **Bst. f** ebenso als wesentliche Einrichtungen zu qualifizieren. Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen wird mit dieser Bestimmung sichergestellt, dass der Ansatz der Richtlinie (EU) 2022/2557 und der Ansatz dieses Gesetzes kohärent sind.

Die zweite Kategorie der Einrichtungen, die wichtigen Einrichtungen, werden in **Abs. 3** geregelt. So sind gemäss **Bst. a** sämtliche Einrichtungen der in Anhang 1

oder 2 aufgeführten Art, die nicht als wesentliche Einrichtungen gelten, als wichtige Einrichtungen zu qualifizieren.

Ebenso wie bei den wesentlichen Einrichtungen, hat die Regierung nach **Bst. b** die Kompetenz, auch sonstige Einrichtungen der in Anhang 1 oder 2 aufgeführten Art, als wichtige Einrichtungen einzustufen. Die Ausführungen zu Abs. 2 Bst. e gelten sinngemäss.

Abs. 4 enthält den Standardhinweis betreffend die Geschlechtsneutralität der verwendeten Personenbezeichnungen.

II. Risikomanagementmassnahmen und Berichtspflichten

A. Wesentliche und wichtige Einrichtungen

Zu Art. 4 – Risikomanagementmassnahmen

Diese Bestimmung legt den Grundsatz fest, wonach wesentliche und wichtige Einrichtungen geeignete und verhältnismässige technische, operative und organisatorische Massnahmen zu ergreifen haben, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie 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 Bestimmungen über die zu treffenden Risikomanagement- und Sicherheitsmassnahmen werden in weiterer Folge in Art. 5 geregelt.

Die Verantwortung für die Gewährleistung der Sicherheit von Netz- und Informationssystemen liegt in erheblichem Masse bei den wesentlichen und wichtigen Einrichtungen. Die wesentlichen und wichtigen Einrichtungen haben die Sicherheit der bei ihren Tätigkeiten verwendeten Netz- und Informationssysteme zu gewährleisten. Hauptsächlich handelt es sich bei diesen Systemen um private

Netz- und Informationssysteme, die entweder von internem IT-Personal der wesentlichen und wichtigen Einrichtung verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Anforderungen an die Risikomanagement- und Sicherheitsmassnahmen sowie der Berichtspflichten im Bereich der Cybersicherheit gemäss diesem Gesetz gilt für die einschlägigen wesentlichen und wichtigen Einrichtungen unabhängig davon, ob diese Einrichtungen ihre Netz- und Informationssysteme intern warten oder deren Wartung ausgliedern.

Zu Art. 5 – Sicherheitsmassnahmen

Abs. 1 entspricht jenem von Art. 21 Abs. 1 Unterabsatz 2 der Richtlinie (EU) 2022/2555. Damit keine unverhältnismässige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Risikomanagement- und Sicherheitsmassnahmen im Bereich der Cybersicherheit in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist. Dabei ist dem bei solchen Massnahmen geltenden neuesten Stand (Stand der Technik) und gegebenenfalls europäischen oder internationalen Normen sowie den Kosten ihrer Umsetzung Rechnung zu tragen.

Die Risikomanagement- und Sicherheitsmassnahmen sollten in einem angemessenen Verhältnis zum Grad der Risikoexposition der wesentlichen oder wichtigen Einrichtung und zu den gesellschaftlichen und wirtschaftlichen Auswirkungen stehen. Bei der Festlegung von Risikomanagement- und Sicherheitsmassnahmen im Bereich der Cybersicherheit, sollte der unterschiedlichen Risikoexposition der betreffenden wesentlichen und wichtigen Einrichtungen gebührend Rechnung getragen werden, wie z. B. der Kritikalität der Einrichtung, den Risiken, einschliesslich der gesellschaftlichen Risiken, denen sie ausgesetzt ist, der Grösse der Einrichtung, der Wahrscheinlichkeit des Auftretens

von Sicherheitsvorfällen und ihrer Schwere, einschliesslich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen.

Abs. 2 legt fest, dass die Sicherheit von Netz- und Informationssystemen auf einem gefahrenübergreifenden Ansatz beruhen muss. Dieser hat darauf abzuzielen, Netz- und Informationssysteme und ihr physisches Umfeld vor Ereignissen wie beispielsweise Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen oder auch vor unbefugtem physischen Zugang und Zugriff zu bzw. auf Informationen und Datenverarbeitungsanlagen einer wesentlichen oder wichtigen Einrichtung und vor der Schädigung dieser Informationen und Anlagen und den entsprechenden Eingriffen zu schützen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können.

Bei den Risikomanagementmassnahmen im Bereich der Cybersicherheit sind daher auch die physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen zu berücksichtigen, indem etwa Massnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen im Einklang mit europäischen und internationalen Normen, wie bspw. denen der Reihe ISO/IEC 27000, einbezogen werden. Die Massnahmen sollten mit der Richtlinie (EU) 2022/2557 im Einklang stehen.

Die Risikomanagement- und Sicherheitsmassnahmen müssen zumindest die in Bst. a bis k aufgeführten umfassen.

Dies sind unter anderem Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme (**Bst. a**) oder auch Massnahmen zur Bewältigung von Sicherheitsvorfällen (**Bst. b**). Letztere umfassen unter anderem Sicherheitsmassnahmen zur Ermittlung der potentiellen Gefahren eines

Sicherheitsvorfalls, zur Verhinderung und Aufdeckung von Sicherheitsvorfällen, zur Reaktion darauf und zur Wiederherstellung danach sowie der Minderung ihrer Folgen.

Ebenso sind Massnahmen zur Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement (**Bst. c**) durch die wesentliche oder wichtige Einrichtung zu implementieren.

Bst. d adressiert die Verwundbarkeit der Lieferketten. Besonders wichtig ist die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten, z. B. Anbietern von Datenspeicherungs- und Datenverarbeitungsdiensten oder Anbietern von verwalteten Sicherheitsdiensten und Softwareherstellern, betreffen. Es häufen sich die Fälle, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Diensten Dritter ausgenutzt werden. Die wesentlichen und wichtigen Einrichtungen sollten daher die Gesamtqualität und Widerstandsfähigkeit der Produkte und Dienste, die darin enthaltenen Risikomanagementmassnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschliesslich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen. Die wesentlichen und wichtigen Einrichtungen sind insbesondere dazu angehalten, Risikomanagement- und Sicherheitsmassnahmen im Bereich der Cybersicherheit in die vertraglichen Vereinbarungen mit ihren direkten Lieferanten und Diensteanbietern einzubeziehen. Diese Einrichtungen könnten auch die Risiken berücksichtigen, die von Lieferanten und Dienstleistern anderer Ebenen ausgehen.

Weiters sind Sicherheitsmassnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschliesslich Management und Offenlegung

von Schwachstellen zu berücksichtigen (**Bst. e**) sowie Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmassnahmen im Bereich der Cybersicherheit zu erarbeiten bzw. festzulegen (**Bst. f**).

Bst. g sieht zudem vor, dass die wesentlichen und wichtigen Einrichtungen eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden, wie beispielsweise Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement oder auch die Sensibilisierung der Nutzer und der Mitarbeitenden durch Schulungen, um das Bewusstsein für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken zu schärfen. Massnahmen für die Cyberhygiene bilden die Grundlage für den Schutz von Netz- und Informationssysteminfrastrukturen, Hardware, Software und Online-Anwendungssicherheit sowie von Geschäfts- oder Endnutzerdaten, derer sich Einrichtungen bedienen.

Es sind Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung zu erarbeiten bzw. festzulegen (**Bst. h**). Hier sollte vor allem der Einsatz von Ende-zu-Ende-Verschlüsselung, insbesondere in der Kommunikation, angestrebt werden.

Ebenso ist die Sicherheit des Personals entsprechend zu berücksichtigen und es sind Konzepte für die Zugriffskontrolle und das Management von Anlagen zu erarbeiten (**Bst. i**).

Abschliessend wird in **Bst. k** festgelegt, dass Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung auf Grundlage einer Risikobewertung zu verwenden sind. Die Multi-Faktor-Authentifizierung (MFA) ist eine zentrale und wichtige Sicherheitsmassnahme, da sie vor allem die Sicherheit

der Benutzerkonten signifikant verbessert. Es werden im Wesentlichen drei Authentifizierungsfaktoren unterschieden: 1.) Etwas, das die zugriffsberechtigte Person weiss. Dies ist häufig ein Passwort oder auch eine Geheimfrage. 2.) Etwas, das die zugriffsberechtigte Person besitzt. Dies kann ein physisches Gerät sein, wie ein Smartphone, ein Sicherheitsschlüssel oder eine Smartcard, die einen zusätzlichen Authentifizierungscode generiert oder empfängt. 3.) Etwas, das die zugriffsberechtigte Person ist. Dies bezieht sich auf biometrische Merkmale, wie Fingerabdrücke, Gesichtserkennung oder Retina-Scans, die eindeutig mit einer Person verknüpft sind. Durch die Verwendung von MFA wird die Wahrscheinlichkeit eines erfolgreichen Angriffs erheblich verringert. Selbst wenn ein Angreifer in der Lage wäre einen Authentifizierungsfaktor zu überwinden, z. B. durch das Ausspionieren des Passworts, muss er immer noch einen weiteren Faktor überwinden, um schliesslich auf ein geschütztes Konto oder ein System zugreifen zu können.

Statt sich auf eine einmalige Authentifizierung zu verlassen, werden bei der kontinuierlichen Authentifizierung das Verhalten des Benutzers, seine Interaktionen und andere Kontextinformationen ständig überwacht, um sicherzustellen, dass der Benutzer weiterhin derjenige ist, für den er sich ausgibt. Dies bietet ebenso eine zusätzliche Schutzebene, indem sie die Sicherheit während der gesamten Interaktion mit dem System oder der Anwendung aufrechterhält, anstatt sich nur auf die anfängliche Authentifizierung zu verlassen.

Wie zu Abs. 2 Bst. d ausgeführt, ist die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten betreffen, von zentraler Bedeutung. **Abs. 3** hebt diese Anforderung nochmals hervor und bestimmt, dass die wesentlichen und wichtigen Einrichtungen bei der Erwägung geeigneter Sicherheitsmassnahmen die spezifischen Schwachstellen sowie die Gesamtqualität der verwendeten Produkte als auch die Cybersicherheitspraxis

ihrer Anbieter und Diensteanbieter, einschliesslich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen müssen (**Bst. a bis d**). Die Einrichtungen sollten grundsätzlich bei der Wahl eines Anbieters erhöhte Sorgfalt walten lassen und die Risiken entsprechend abwägen.

Mit **Abs. 4** soll sichergestellt werden, dass die wesentliche und wichtige Einrichtung gegebenenfalls die erforderlichen, angemessenen und verhältnismässigen Korrekturmassnahmen ergreift, sofern sie feststellt, dass den erforderlichen Risiko- und Sicherheitsmassnahmen nicht nachgekommen wird.

Abs. 5 entspricht dem Lex specialis Vorbehalt des Art. 4 der Richtlinie (EU) 2022/2555. Wenn wesentliche oder wichtige Einrichtungen gemäss den Bestimmungen eines sektorspezifischen Rechtsakts der Union entweder Risikomanagement- oder andere Sicherheitsmassnahmen im Bereich der Cybersicherheit ergreifen oder erhebliche Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen zumindest gleichwertig sind, finden diese Bestimmungen, einschliesslich der Bestimmungen über Aufsicht und Durchsetzung, keine Anwendung auf solche Einrichtungen.

Die Verordnung (EU) 2022/2554 (DORA) kann gegenständlich als sektorspezifischer Rechtsakt der Union in Bezug auf Finanzunternehmen betrachtet werden. Anstelle der Bestimmungen dieses Gesetzes gelten für Finanzunternehmen die Bestimmungen der Verordnung (EU) 2022/2554, die sich auf Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT), das Management von IKT-bezogenen Vorfällen und insbesondere die Meldung von schwerwiegenden IKT-bezogenen Vorfällen sowie die Prüfung der digitalen Betriebsstabilität, Vereinbarungen über den Informationsaustausch und Risiken durch IKT-Drittanbieter beziehen. Weiters finden jene Bestimmungen dieses Gesetzes, die sich auf die Aufsicht und

Durchsetzung beziehen, auf Finanzunternehmen – sofern sie unter die Verordnung (EU) 2022/2554 fallen – keine Anwendung.

Abs. 6 enthält eine Verordnungskompetenz für die Regierung, das Nähere über die Risikomanagement- und Sicherheitsmassnahmen mittels Verordnung zu regeln.

Zu Art. 6 – Berichtspflichten

Ein proaktiver Ansatz gegen Cyberbedrohungen ist ein wesentliches Element der Cybersicherheit und ein wichtiges Ziel ist es, durch präventive und wirksame Massnahmen zu verhindern, dass Cyberbedrohungen in Sicherheitsvorfälle münden, die erhebliche materielle oder immaterielle Schäden verursachen können. Zu diesem Zweck ist die Meldung von Cyberbedrohungen, von Sicherheitsvorfällen und von beinahe Sicherheitsvorfällen von zentraler Bedeutung. Zu diesem Zweck wird sämtlichen Einrichtungen nahegelegt, Cyberbedrohungen – ungeachtet einer allfälligen Verpflichtung – auch auf freiwilliger Basis zu melden.

Mit Art. 6 wird die Berichtserstattungspflicht der Richtlinie (EU) 2022/2555 umgesetzt. Der in der Richtlinie vorgegebene mehrstufige Ansatz für die Meldung von Sicherheitsvorfällen wurde in diese Gesetzesvorlage übernommen. Damit soll die Balance zwischen einer zeitnahen Meldung einerseits – die einer potenziellen Ausbreitung erheblicher Sicherheitsvorfälle entgegenwirkt und den wesentlichen und wichtigen Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten – und einer detaillierten Meldung andererseits – bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Einrichtungen und ganze Sektoren ihre Widerstandsfähigkeit gegenüber Cyberangriffen im Laufe der Zeit verbessern können – hergestellt.

Abs. 1 regelt diesen mehrstufigen Ansatz. So haben wesentliche und wichtige Einrichtungen nach **Bst. a** unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme eines erheblichen Sicherheitsvorfalls, der Stabsstelle Cyber-Sicherheit eine Frühwarnung zu senden, 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. Die Verpflichtung die Frühwarnung oder auch die anschliessenden Meldungen eines Sicherheitsvorfalls an die Stabsstelle Cyber-Sicherheit zu übermitteln, sollte nicht dazu führen, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen – was Vorrang hat – abziehen muss, sodass diese Verpflichtung die betroffene Einrichtungen zusätzlich beeinträchtigt.

Mit **Bst. b** wird festgelegt, dass unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall an die Stabsstelle Cyber-Sicherheit zu erfolgen hat. Dabei werden gegebenenfalls die unter Bst. a genannten Informationen aktualisiert und eine erste Bewertung des erheblichen Sicherheitsvorfalls angegeben.

Abs. 2 regelt die Möglichkeit der Stabsstelle Cyber-Sicherheit, nach einem erheblichen Sicherheitsvorfall von der betroffenen wesentlichen oder wichtigen Einrichtung einen Zwischenbericht über relevante Statusaktualisierungen zu verlangen.

Abs. 3 legt fest, dass spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls die betroffene wesentliche oder wichtige Einrichtung der Stabsstelle Cyber-Sicherheit einen Fortschrittsbericht im Falle eines andauernden Sicherheitsvorfalls oder einen Abschlussbericht nach Abschluss der Behandlung

des Sicherheitsvorfalls zu übermitteln hat. Der Inhalt des Abschlussberichts wird in Abs. 4 geregelt.

Abs.4 enthält in den Bst. a bis d eine Auflistung über den im Abschlussbericht geforderten Inhalt. Dies ist zumindest eine ausführliche Beschreibung des Sicherheitsvorfalls, einschliesslich seines Schweregrads und seiner Auswirkungen (**Bst. a**), Angaben zur Art der Bedrohung bzw. der dieser zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat (**Bst. b**), Angaben zu den getroffenen und laufenden Abhilfemassnahmen (**Bst. c**) sowie gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls (**Bst. d**).

Abs. 5 sieht zusätzlich zur Berichtspflicht an die Stabsstelle Cyber-Sicherheit eine Verpflichtung zur unverzüglichen Information von Empfängern der Dienste der wesentlichen oder wichtigen Einrichtungen vor, sofern diese mit vernünftigem Aufwand erhoben werden können. Die Formulierung in Abs. 5 entspricht jener aus Art. 21 Abs. 1 2. Satz sowie Art. 21 Abs. 2 1. Satz der Richtlinie (EU) 2022/2555. So hat die von einem erheblichen Sicherheitsvorfall betroffene wesentliche oder wichtige Einrichtung gegebenenfalls jene Empfänger ihrer Dienste unverzüglich über den erheblichen Sicherheitsvorfall zu informieren, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Sprich, die Empfänger der Dienste werden darüber informiert, dass ein erheblicher Sicherheitsvorfall stattgefunden hat und durch die Nutzung des Dienstes das Risiko einer Beeinträchtigung besteht. Wesentliche und wichtige Einrichtungen informieren potenziell von einer erheblichen Cyberbedrohung betroffene Empfänger oder Nutzer unverzüglich, wenn diese Bedrohung wahrscheinlich eintreten wird. Dabei teilen die wesentlichen und wichtigen Einrichtungen gegebenenfalls den Empfängern ihrer Dienste unverzüglich alle Massnahmen oder Abhilfemassnahmen mit, die sie ergreifen können, um die sich aus einer erheblichen Cyberbedrohung ergebenden

Risiken zu mindern. Die Informationspflicht sollte nach besten Kräften erfüllt werden, sollte die betroffene Einrichtung jedoch nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmassnahmen zu ergreifen, um jedwede derartige Bedrohung bei den Empfängern zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über erhebliche Cyberbedrohungen für die Empfänger und Nutzer sind kostenlos abzugeben, und die Informationen sollten in leicht verständlicher Sprache abgefasst werden.

Abs. 6 entspricht im Wortlaut Art. 5 Abs. 3 CSG und bleibt unverändert. Die Stabsstelle Cyber-Sicherheit hat für Meldungen ein Online-Formular auf ihrer Internetseite zur Verfügung gestellt. Dieses ist direkt auf der Startseite unter https://scs.llv.li abrufbar.

Abs. 7 entspricht im Wortlaut Art. 5 Abs. 6 CSG. Der Lex specialis Vorbehalt wurde unverändert aus dem bestehenden CSG übernommen und hat keine Anpassung erfahren. Er setzt Art. 4 der Richtlinie (EU) 2022/2555 entsprechend um.

Die Regierung hat gemäss **Abs. 8** eine Verordnungskompetenz, um die Berichtspflicht näher zu präzisieren und auszugestalten. Die Bestimmung entspricht unverändert Art. 5 Abs. 7 CSG.

Zu Art. 7 – Information der Öffentlichkeit

Mit der gegenständlichen Totalrevision werden zwei bereits existierende Bestimmungen im CSG in einer eigenen Bestimmung zusammengefasst. **Bst. a** entspricht im Wesentlichen der Bestimmung Art. 5 Abs. 5 CSG und Art. 7 Abs. 2 Bst. a CSG. Nach einer Meldung an die Stabsstelle Cyber-Sicherheit und Anhörung der betreffenden Einrichtung kann die Stabsstelle die Öffentlichkeit über konkrete Sicherheitsvorfälle informieren oder verlangen, dass die Einrichtung dies unternimmt, sofern die Sensibilisierung der Öffentlichkeit zur Verhütung von

Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist. **Bst. b** entspricht im Kern Art. 7 Abs. 2 Bst. b CSG. So ist die Offenlegung eines Sicherheitsvorfalls möglich, sofern dies im öffentlichen Interesse liegt.

B. Andere Einrichtungen

Zu Art. 8 – Freiwillige Meldung

Die freiwillige Meldung findet sich bereits in Art. 8 CSG. In **Abs. 1** wurden die Begrifflichkeiten entsprechend der Richtlinie (EU) 2022/2555 angepasst, sodass jetzt von Einrichtungen und nicht mehr von Betreibern wesentlicher Dienste gesprochen wird. Durch die begriffliche Anpassung eröffnet es sich zudem einem noch grösseren Betroffenenkreis freiwillige Meldungen an die Stabsstelle Cyber-Sicherheit übermitteln zu können. Inhaltlich bleibt die Bestimmung unverändert. **Abs. 2** wurde im Wortlaut ident übernommen und entspricht dem Art. 8 Abs. 2 CSG.

III. Organisation und Durchführung

A. Allgemeines

Zu Art. 9 – Zuständigkeit

Die Bestimmung bleibt in der gegenständlichen Totalrevision unangetastet und entspricht dem Art. 9 CSG.

Zu Art. 10 – Amtsgeheimnis

Ebenso bleibt diese Bestimmung in der gegenständlichen Totalrevision unangetastet und entspricht dem Art. 10 CSG.

Zu Art. 11 – Verarbeitung und Offenlegung personenbezogener Daten

Abs. 1 und **Abs. 2** entsprechen, mit Ausnahme der Ergänzung betreffend die Verarbeitung von besonderen Kategorien personenbezogener Daten in Abs. 1

sowie der Anpassung des Verweises in Abs. 2 Bst. a, hier wurde die Richtlinie (EU) 2016/1148 durch die Richtlinie (EU) 2022/2555 ersetzt, Art. 11 Abs. 1 und 2 CSG.

Die Ergänzung betreffend die Verarbeitung der besonderen Kategorien personenbezogener Daten basiert auf Erwägungsgrund 121 der Richtlinie (EU) 2022/2555. Es wird mit der Ergänzung der Stabsstelle Cyber-Sicherheit ermöglicht, besondere Kategorien personenbezogener Daten gemäss Art. 9 der Verordnung (EU) 2016/679 zu verarbeiten, soweit dies zur Gewährleistung der Sicherheit der Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen erforderlich und verhältnismässig ist.

Abs. 3 schafft für sämtliche Einrichtungen eine Rechtsgrundlage für den freiwilligen Austausch von Informationen in Zusammenhang mit Cybersicherheit untereinander. Der Informationsaustausch im Hinblick auf die Verhütung, Erkennung, Identifizierung, Eindämmung, Analyse und Bewältigung von Sicherheitsvorfällen, zur Sensibilisierung für spezifische Cyberbedrohungen, im Zusammenhang mit der Behebung von Schwachstellen und der koordinierten Offenlegung von Schwachstellen, von Kompromittierungsindikatoren (IOCs), von Taktiken, Vorgehensweisen und Verfahren erfordert regelmässig die Verarbeitung bestimmter Kategorien personenbezogener Daten wie etwa IP-Adressen, URL-Adressen, Domänennamen oder E-Mail-Adressen, sofern diese als personenbezogene Daten zu qualifizieren sind.

Gemäss Abs. 3 können die Einrichtungen Informationen betreffend die Cybersicherheit austauschen, insbesondere über Cyberbedrohungen (**Bst. a**), Schwachstellen (**Bst. b**), Taktiken, Techniken und Verfahren, sogenannte TTPs (**Bst. c**), Kompromittierungsindikatoren (**Bst. d**), Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen (**Bst. e**) sowie Beinahe-Vorfälle (**Bst. f**) verarbeiten.

Da Cyberbedrohungen komplexer und technisch ausgereifter werden, hängen eine gute Erkennung dieser Bedrohungen und entsprechende Präventionsmassnahmen in hohem Masse von einem regelmässigen Informationsaustausch zwischen den Einrichtungen über Bedrohungen und Schwachstellen ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen, wodurch Einrichtungen Bedrohungen abwehren können, bevor diese in Sicherheitsvorfälle münden, und in der Lage sind, die Auswirkungen von Sicherheitsvorfällen besser einzudämmen und effizienter zu reagieren.

Die Zwecke des Informationsaustauschs nach Abs. 3 werden in **Abs. 4** aufgelistet. So erfolgt der freiwillige Informationsaustausch der Einrichtungen, um Sicherheitsvorfälle zu verhindern, aufzudecken, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen (**Bst. a**) oder um das Cybersicherheitsniveau zu erhöhen (**Bst. b**). Ein legitimer Zweck gemäss Bst. b ist unter anderem das Leisten von Aufklärungsarbeit über Cyberbedrohungen (**Ziff. 1**). Ebenso soll durch den Informationsaustausch das Cybersicherheitsniveau erhöht werden, indem die Fähigkeit von Cyberbedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird (**Ziff. 2**), die Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden (**Ziff. 3**), und die gemeinsame Forschung im Bereich Cyberbedrohung zwischen öffentlichen und privaten Einrichtungen gefördert wird (**Ziff. 4**).

Die Einrichtungen werden ermutigt und von der Stabsstelle Cyber-Sicherheit auch dabei unterstützt, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeiten verbessern, Sicherheitsvorfälle angemessen zu verhindern, zu

erkennen, auf sie zu reagieren, sie zu bewältigen oder in ihrer Wirkung zu begrenzen.

Die Stabsstelle Cyber-Sicherheit wird Einrichtungen, wie jene, die Cybersicherheitsdienste und -forschung anbieten, sowie einschlägige Einrichtungen, die nicht unter dieses Gesetz fallen, ebenso aktiv unterstützen und dazu anhalten, sich an Vereinbarungen zum Austausch von Informationen über Cybersicherheit zu beteiligen.

B. Stabsstelle Cyber-Sicherheit

Zu Art. 12 – Zuständigkeit

Abs. 1 und **Abs. 2** entsprechen, mit Ausnahme der Anpassungen der Richtlinien-Verweise, Richtlinie (EU) 2016/1148 wurde jeweils durch die Richtlinie (EU) 2022/2555 ersetzt, dem Wortlaut von Art. 12 Abs. 1 und 2 CSG.

Der zusätzliche **Abs. 3** legt fest, dass die Stabsstelle Cyber-Sicherheit die für das Management von Cybersicherheitsvorfällen grossen Ausmasses und Krisen zuständige Behörde nach Art. 9 Abs. 1 der Richtlinie (EU) 2022/2555 ist. Liechtenstein hat die Kapazitäten, Mittel und Verfahren, welche im Fall einer Krise eingesetzt werden können, zu ermitteln. Die Stabsstelle Cyber-Sicherheit koordiniert diese Ermittlung der erwähnten Kapazitäten, Mittel und Verfahren sowie die Erstellung und Verabschiedung eines nationalen Plans 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 werden insbesondere festgelegt: die Ziele der nationalen Vorsorgenmassnahmen und -tätigkeiten; die Aufgaben und Zuständigkeiten der Behörden für das Cyberkrisenmanagement; die Verfahren für das Cyberkrisenmanagement, einschliesslich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und die Kanäle für

den Informationsaustausch; die nationalen Vorsorgemassnahmen, einschliesslich Übungen und Ausbildungsmassnahmen; die einschlägigen öffentlichen und privaten Interessenträger und die betroffene Infrastruktur, die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich Liechtenstein wirksam am koordinierten Management von Cybersicherheitsvorfällen grossen Ausmasses und Krisen auf EWR-Ebene beteiligen und dieses unterstützen kann.

Der zusätzliche **Abs. 4** bestimmt, dass die Stabsstelle Cyber-Sicherheit die nationale Behörde für Cybersicherheitszertifizierungen nach Art. 58 Abs. 1 der Verordnung (EU) 2019/881 ist und als solche die Aufgaben und Befugnisse nach Art. 58 Abs. 7 und 8 der Verordnung (EU) 2019/881 wahrnimmt.

Gemäss Verordnung (EU) 2019/881, auch bekannt als die Cybersecurity Act (CSA), wurde ein europäischer Rahmen für die Zertifizierung von Cybersicherheit geschaffen. Ziel ist es, das Vertrauen in digitale Dienste und Produkte zu stärken und die digitale Wirtschaft im EWR zu unterstützen. Eine Cybersicherheitszertifizierung ist eine formelle Anerkennung und bestätigt, dass ein bestimmtes IKT-Produkt, ein IKT-Dienst oder ein IKT-Prozess die in einem sogenannten Schema festgehaltenen Anforderungen erfüllt. Zudem können Zertifizierungen dazu beitragen, die Einhaltung von gesetzlichen und regulatorischen Anforderungen zu gewährleisten und nachzuweisen.

Die nationale Behörde für Cybersicherheitszertifizierungen beaufsichtigt unter anderem die sich aus der Verordnung (EU) 2019/881 ergebenden Verpflichtungen der verschiedensten Beteiligten, wie z. B. der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen oder der Konformitätsbewertungsstellen. Die nationale Behörde spielt eine wichtige Rolle bei der Umsetzung der Cybersicherheitszertifizierung und die Verpflichtung zur Benennung einer nationalen Behörde ergibt sich aus den zitierten EU-Rechtsakten.

Doch Aufgrund ihrer Grösse und dem erwarteten Aufwand wird die Stabsstelle Cyber-Sicherheit im Zusammenhang mit Cybersicherheitszertifizierungen Partnerschaften eingehen. Entsprechende Abklärungen laufen und erste Ergebnisse werden für das erste Halbjahr 2024 erwartet.

Zu Art. 13 – Aufgaben

Die Aufgaben der Stabsstelle Cyber-Sicherheit gemäss Abs. 1 sind sowohl strategischer als auch operativer Natur und umfassen Tätigkeiten von der Überprüfung der Risikomanagement- und Sicherheitsmassnahmen sowie die Einhaltung der Berichtspflichten (Bst. a), über die Koordination einer NIS-Strategie (Bst. p), bis zur Vertretung Liechtensteins in Gremien im EWR und in internationalen Gremien (Bst. q).

Im Wesentlichen entspricht Abs. 1 dem Art. 13 Abs. 1 CSG, wobei bestehende Aufgaben vor allem begrifflich angepasst und aufgrund der Umsetzung der Richtlinie (EU) 2022/2555 weitere zusätzliche Aufgaben hinzugekommen sind.

Bst. a hebt einen wesentlichen Teil der Überwachung hervor, welche die Überprüfung von Risikomanagement- und Sicherheitsmassnahmen (Art. 4 und 5) und die Einhaltung der Berichtspflichten (Art. 6) betrifft. Die Bestimmung entspricht – mit Ausnahme redaktioneller Anpassungen – unverändert Art. 13 Abs. 1 Bst. a CSG. Es sind keine periodischen Kontrollen seitens der Stabsstelle Cyber-Sicherheit vorgegeben. Die wesentlichen und wichtigen Einrichtungen sollen mit der Stabsstelle Cyber-Sicherheit vielmehr im engen regelmässigen Austausch in Bezug auf die Einhaltung der entsprechenden Bestimmungen stehen. Weitere Ausführungen zur Kontrolltätigkeit finden sich in den Erläuterungen zu Art. 17.

Bst. b legt fest, dass die Einrichtung und Koordination des Computer-Notfallteams (CSIRT) nach Art. 18 zur Gewährleistung der Sicherheit von Netz- und

Informationssystemen eine weitere Aufgabe der Stabsstelle Cyber-Sicherheit darstellt. Diese Bestimmung entspricht unverändert Art. 13 Abs. 1 Bst. b CSG.

Insbesondere zwecks der Erstellung von Lagebildern und zur Durchführung von Analysen ist es die Aufgabe der Stabsstelle Cyber-Sicherheit gemäss **Bst. c**, Meldungen über Risiken oder Sicherheitsvorfälle entgegenzunehmen und zu analysieren. Diese Bestimmung entspricht unverändert Art. 13 Abs. 1 Bst. c CSG.

Bst. d ergänzt die zuvor erwähnte Aufgabe mit jener, dass die Erstellung und Weitergabe von relevanten Informationen, die beispielsweise nicht auf Meldungen nach Art. 6 und Art. 8 basieren, zur Gewährleistung der Sicherheit von Netz- und Informationssystemen oder zur Vorbeugung von Sicherheitsvorfällen ebenso eine Aufgabe der Stabsstelle Cyber-Sicherheit darstellt. Die Bestimmung entspricht unverändert Art. 13 Abs. 1 Bst. d CSG.

Bst. e regelt, dass die Stabsstelle Cyber-Sicherheit die wesentlichen und wichtigen Einrichtungen sowie Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, in einer Liste festhält. Regelmässig, jedoch mindestens alle zwei Jahre wird diese Liste der wesentlichen und wichtigen Einrichtungen durch die Stabsstelle überprüft und bei Bedarf aktualisiert. Mit dieser Aufgabe wird Art. 3 Abs. 3 der Richtlinie (EU) 2022/2555 umgesetzt.

Dabei arbeitet die Stabsstelle Cyber-Sicherheit mit dem Amt für Bevölkerungsschutz zusammen. Mit dieser Liste verschafft sich die Stabsstelle Cyber-Sicherheit einen Überblick über die in den Anwendungsbereich dieser Vorlage fallenden Einrichtungen.

Abweichend vom bisherigen Art. 13 Abs. 1 Bst. e CSG und der Richtlinie (EU) 2016/1148 verlangt die Bestimmung in Bst. e nicht mehr, dass die Stabsstelle Cyber-Sicherheit die wesentlichen und wichtigen Einrichtungen von sich aus ermittelt. Dies bedeutet, dass eine Einrichtung von der Stabsstelle Cyber-

Sicherheit nicht zwingend kontaktiert werden muss, um als wesentliche oder wichtige Einrichtung im Sinne dieser Vorlage zu gelten oder in den Anwendungsbereich dieser Vorlage zu fallen. Die Stabsstelle Cyber-Sicherheit wird jedoch bestehende Register und bisherige Ermittlungen für die Erstellung der gegenständlichen Liste nutzen.

Der Zweck der Liste besteht unter anderem darin, die Beaufsichtigung wesentlicher und wichtiger Einrichtungen, die in den Anwendungsbereich dieser Vorlage fallen, zu unterstützen. Somit sollten keine Einrichtungen in der Liste aufgenommen werden, für die sektorspezifische EWR-Rechtsakt in Bezug auf das Risikomanagement und der Berichtspflichten im Bereich der Cybersicherheit, einschliesslich der Bestimmungen über die Beaufsichtigung und Durchsetzung, gelten würde. Da die DORA als sektorspezifischer Rechtsakt der Union gilt (siehe Art. 1 Abs. 2 der Verordnung (EU) 2022/2554 und Erwägungsgrund 28 der Richtlinie (EU) 2022/2555), werden folglich jene Einrichtungen die unter diese Verordnung fallen nicht in der gegenständlichen Liste geführt.

Bst. f bestimmt, dass die Stabsstelle Cyber-Sicherheit ebenso eine Liste über Vertreter gemäss Art. 3 Abs. 1 Ziff. 35 führt und diesbezügliche Nennungen entgegennimmt.

Eine weitere Aufgabe der Stabsstelle Cyber-Sicherheit gemäss **Bst. g** ist die Förderung der Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

Nach **Bst. h** sind die Unterrichtung und Weiterleitung von durch wesentliche und wichtige Einrichtungen bereitgestellten Informationen an den bzw. die anderen betroffenen EWR-Mitgliedstaaten eine weitere Aufgabe der Stabsstelle Cyber-Sicherheit. Die Unterrichtung und Weiterleitung erfolgt jedoch lediglich in jenen

Fällen, in denen ein Sicherheitsvorfall grenzüberschreitende Auswirkungen in einem oder mehreren anderen EWR-Mitgliedstaaten hat. Die Bestimmung entspricht sinngemäss Art. 13 Abs. 1 Bst. f CSG.

Bst. i entspricht sinngemäss Art. 13 Abs. 1 Bst. g CSG. Der Stabsstelle Cyber-Sicherheit obliegt nach Bst. i die Koordination der öffentlich-privaten Zusammenarbeit im Bereich der Cybersicherheit. Diese zentrale Schnittstellenfunktion des Landes zu Gesellschaft, Wirtschaft und Wissenschaft im Bereich der Cybersicherheit nimmt die Stabsstelle Cyber-Sicherheit beispielsweise in Form des Nationalen Koordinierungszentrums Cybersicherheit (NCC-LIE) im Sinne der Verordnung (EU) 2021/887[3] wahr. Mit dieser Bestimmung wird – wie schon im CSG – die Verordnung (EU) 2021/887 entsprechend durchgeführt.

Bst. k legt fest, dass die Unterrichtung sowie die Sensibilisierung der Öffentlichkeit über Sicherheitsvorfälle sowie die Veröffentlichung allgemeiner Informationen im Zusammenhang mit der Cybersicherheit weitere Aufgaben der Stabsstelle Cyber-Sicherheit sind. Für die Öffentlichkeitsarbeit bedient sich die Stabsstelle verschiedenster Kanäle, wie beispielsweise der eigenen Internetseite oder auch Newslettern. Sensibilisierung für Cybersicherheit und Cyberhygiene sind von entscheidender Bedeutung, um das Cybersicherheitsniveau zu erhöhen, insbesondere angesichts der wachsenden Zahl vernetzter Geräte, die zunehmend bei Cyberangriffen eingesetzt werden. Bst. k entspricht – mit Ausnahme redaktioneller bzw. begrifflicher Anpassungen –Art. 13 Abs. 1 Bst. h CSG.

Die Stabsstelle Cyber-Sicherheit arbeitet mit öffentlichen Stellen, insbesondere der Landespolizei, der Staatsanwaltschaft, der Datenschutzstelle, dem Amt für Informatik, dem Amt für Kommunikation, dem Amt für Bevölkerungsschutz, dem

[3] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. 202 vom 8.6.2021, S. 1).

Amt für Hochbau und Raumplanung, dem Amt für Tiefbau und Geoinformation, der Stabsstelle FIU und der Finanzmarktaufsicht Liechtenstein zusammen und tauscht zum Zweck des Schutzes der Netz- und Informationssysteme relevante Informationen aus (**Bst. l**). Bst l entspricht Art. 13 Abs. 1 Bst. i CSG, wobei das Amt für Hochbau und Raumplanung sowie das Amt für Tiefbau und Geoinformation aufgenommen wurden. Das Amt für Hochbau und Raumplanung ist jene Amtsstelle der LLV, die den Themenbereich der Zivilluftfahrt betreut und auch einzelne dem Amt konkret zugewiesene Geschäfte der Luftfahrtgesetzgebung vollzieht. Die Liste ist nicht abschliessend. Die Stabsstelle Cyber-Sicherheit wird neben den zuvor erwähnten ebenso mit anderen Stellen entsprechende Kontakte pflegen und Informationen austauschen.

Bst. m bestimmt, dass die Stabsstelle Cyber-Sicherheit mit dem Landesführungsstab zusammenarbeitet und die Ausarbeitung eines nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle grossen Ausmasses und Krisen koordiniert. Es handelt sich dabei um eine neue Aufgabe, welche mit der Umsetzung der Richtlinie (EU) 2022/2555 auf die Stabsstelle zukommt. Die Bestimmung setzt Art. 9 Abs. 4 der Richtlinie (EU) 2022/2555 national um.

Der Plan für die Reaktion auf Cybersicherheitsvorfälle grossen Ausmasses und Krisen legt insbesondere Folgendes fest: die Ziele der nationalen Vorsorgenmassnahmen und -tätigkeiten; die Aufgaben und Zuständigkeiten der Behörden für das Cyberkrisenmanagement; die Verfahren für das Cyberkrisenmanagement, einschliesslich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und die Kanäle für den Informationsaustausch; die nationalen Vorsorgemassnahmen, einschliesslich Übungen und Ausbildungsmassnahmen sowie die einschlägigen öffentlichen und privaten Interessenträger und die betroffene Infrastruktur.

Gegenständlich arbeitet die Stabsstelle Cyber-Sicherheit eng mit bereits bestehenden Strukturen, wie beispielsweise dem Amt für Bevölkerungsschutz, zusammen.

Eine weitere Aufgabe der Stabstelle Cyber-Sicherheit ist die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch, wie etwa im Falle der Amtshilfe oder eines erheblichen Sicherheitsvorfalls oder bei einem Cybersicherheitsvorfall grossen Ausmasses, von dem zwei oder mehr EWR-Mitgliedstaaten betroffen sind, mit den zuständigen Behörden und Stellen in anderen EWR-Mitgliedstaaten, der ENISA, der Kooperationsgruppe, dem EU-CyCLONe und dem CSIRTs-Netzwerk (**Bst. n**).

Neben den EWR-Mitgliedstaaten pflegt die Stabsstelle Cyber-Sicherheit auch Kontakte mit vertrauenswürdigen Drittstaaten, insbesondere mit der Schweiz. Gemäss **Bst. o** ist die grenzüberschreitende Zusammenarbeit und der Informationsaustausch im Bereich der Cybersicherheit mit öffentlichen und nicht öffentlichen Stellen sowie Behörden in Drittstaaten eine weitere Aufgabe der Stabsstelle. Die Stabsstelle Cyber-Sicherheit kann mit Drittländern zusammenarbeiten und Tätigkeiten durchführen, die zur Aufgabenerfüllung als angemessen erachtet werden, wozu auch der Informationsaustausch über Cyberbedrohungen, Vorfälle, Schwachstellen, Instrumente und Methoden, Taktiken, Techniken und Verfahren, die Vorsorge und Übungen im Hinblick auf das Krisenmanagement im Cyberbereich, Schulungen, die Vertrauensbildung und Vereinbarungen über den strukturierten Informationsaustausch gehören. Die Bestimmung entspricht – mit Ausnahme redaktioneller bzw. begrifflicher Anpassungen – Art. 13 Abs. 1 Bst. l CSG.

Bst. p entspricht im Kern Art. 13 Abs. 1 Bst. m CSG. Bst. p adressiert die nationale Strategie zur Cybersicherheit (Art. 19). Gemäss Art. 7 Abs. 1 der Richtlinie (EU) 2022/2555 erlässt jeder EWR-Mitgliedstaat 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. Es ist Aufgabe der Stabsstelle Cyber-Sicherheit, die Erstellung der nationalen Cybersicherheitsstrategie zu koordinieren.

Die Stabsstelle Cyber-Sicherheit ist nach **Bst. q** die Vertretung von Liechtenstein in der Kooperationsgruppe, dem CSIRTs-Netzwerk, dem EU-CyCLONe, der Europäischen Gruppe für die Cybersicherheitszertifizierung sowie in anderen grenzüberschreitenden Gremien im EWR und internationalen Gremien für die Cybersicherheit. Die Bestimmung entspricht Art. 13 Abs. 1 Bst. n CSG, wobei weitere internationale Gruppen und Gremien, wie bspw. EU-CyCLONe oder auch die Europäische Gruppe für die Cybersicherheitszertifizierung mit der Umsetzung der Richtlinie (EU) 2022/2555 bzw. der Durchführung der Verordnung (EU) 2019/881 hinzugekommen sind.

Abschliessend wird mit **Bst. r** festgelegt, dass die Stabsstelle Cyber-Sicherheit an sogenannten Peer Reviews gemäss Art. 19 der Richtlinie (EU) 2022/2555 teilnimmt. Die Methode und die organisatorischen Aspekte der Peer Reviews werden durch die Kooperationsgruppe festgelegt, um aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu stärken, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die für die Umsetzung der Richtlinie (EU) 2022/2555 erforderlichen Cybersicherheitsfähigkeiten zu verbessern. Die Teilnahme an Peer Reviews ist freiwillig und werden von Sachverständigen für Cybersicherheit durchgeführt.

Abs. 2 entspricht unverändert Art. 13 Abs. 2 CSG und erlaubt es der Stabsstelle Cyber-Sicherheit nach Rücksprache mit dem zuständigen Regierungsmitglied mit anderen in- und ausländischen Behörden Vereinbarungen über die Modalitäten der Zusammenarbeit abzuschliessen sowie zur Aufgabenerfüllung mit Privaten im

Rahmen von öffentlich-privaten Partnerschaften zusammenzuarbeiten. Öffentlich-private Partnerschaften (ÖPP) im Bereich der Cybersicherheit können einen angemessenen Rahmen für den Wissensaustausch, die Weitergabe von bewährten Verfahren und die Schaffung einer gemeinsamen Verständnisebene zwischen den Beteiligten bieten. Die Stabsstelle Cyber-Sicherheit kann mit einer ÖPP das Fachwissen privatwirtschaftlicher Einrichtungen nutzen, um Dienste und Prozesse weiterzuentwickeln, unter anderem in den Bereichen Informationsaustausch, Frühwarnungen, Übungen zu Cyberbedrohungen und -vorfällen, Krisenmanagement und Resilienzplanung.

Mit **Abs. 3** bekommt die Regierung eine Verordnungskompetenz und kann das Nähere über die Aufgaben der Stabsstelle Cyber-Sicherheit mit Verordnung regeln. Diese Bestimmung entspricht unverändert Art. 13 Abs. 3 CSG.

Zu Art. 14 – Befugnisse gegenüber wesentlichen und wichtigen Einrichtungen

Neben den Aufgaben nach Art. 13 wird die Stabsstelle Cyber-Sicherheit mit den zur Erfüllung ihrer Aufgaben erforderlichen Befugnissen gegenüber wesentlichen und wichtigen Einrichtungen ausgestattet.

Abs. 1 entspricht – mit Ausnahme redaktioneller bzw. begrifflicher Anpassungen – Art. 14 Abs. 1 CSG. Die Stabsstelle Cyber-Sicherheit kann demnach bei der Wahrnehmung ihrer Aufgaben nach dieser Vorlage von den wesentlichen und wichtigen Einrichtungen verlangen, dass sie ihr die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, zur Verfügung stellen (**Bst. a**), Nachweise für die wirksame Umsetzung der Sicherheitsmassnahmen erbringen (**Bst. b**) sowie Informationen, insbesondere technische und statistische Daten, zu statistischen Zwecken oder für die Erstellung konkreter Lagebilder unentgeltlich offenlegen (**Bst. c**).

Mit der Umsetzung der Richtlinie (EU) 2022/2555 erhält die Stabsstelle Cyber-Sicherheit weitere Befugnisse.

So kann die Stabsstelle Cyber-Sicherheit nach **Abs. 2** von wesentlichen und wichtigen Einrichtungen bestimmte Angaben (Bst. a bis f) verlangen. Damit wird Art. 3 Abs. 4 der Richtlinie (EU) 2022/2555 umgesetzt und die Angaben dienen vor allem der Erstellung der Liste gemäss Art. 13 Abs. 1 Bst. e.

Abs. 3 sieht weiters vor, dass wesentliche und wichtige Einrichtungen der Stabsstelle Cyber-Sicherheit zwecks Registrierung die Angaben nach Abs. 2. übermitteln. Die Übermittlung hat unverzüglich, in jedem Fall aber innerhalb von vier Wochen ab Inkrafttreten dieses Gesetzes zu erfolgen. Ebenso informieren wesentliche und wichtige Einrichtungen die Stabsstelle Cyber-Sicherheit unverzüglich über jede Änderung der Angaben nach Abs. 2, in jedem Fall aber innerhalb von zwei Wochen ab dem Tag der Änderung.

Diese Bestimmung legt fest, dass abweichend vom aktuellen CSG nicht mehr die Stabsstelle Cyber-Sicherheit die kritische Infrastruktur ermittelt, sondern dass die wesentlichen und wichtigen Einrichtungen dies aus Eigenem zu prüfen haben. Die Einrichtungen prüfen, ob sie allenfalls unter das Cyber-Sicherheitsgesetz fallen und teilen dies der Stabsstelle Cyber-Sicherheit mit. Neben der Ersterfassung und Registrierung haben die wesentlichen und wichtigen Einrichtungen jede Änderung der Stabsstelle Cyber-Sicherheit mitzuteilen. Neben einschlägigen Informationen und Leitlinien zur Prüfung des Anwendungsbereichs wird die Stabsstelle Cyber-Sicherheit für die Registrierung und die Änderung der Angaben entsprechende elektronische Formulare auf ihrer Internetseite zur Verfügung stellen.

Mit **Abs. 4** bekommt die Stabsstelle Cyber-Sicherheit die Befugnis, wesentliche oder wichtige 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. Damit wird Art. 32 Abs. 4 Bst. e der Richtlinie (EU) 2022/2555 national umgesetzt.

Mit **Abs. 5** bekommt die Stabsstelle Cyber-Sicherheit die Befugnis, wesentliche oder wichtige Einrichtungen in begründeten Fällen zu verpflichten, für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung der Art. 4 bis 6 dieser Vorlage durch die betreffenden Einrichtungen überwacht. Die Verpflichtung muss in allen Fällen begründet sein. Beispielsweise wenn nachweislich Anhaltspunkte dafür vorliegen, dass gegen die Bestimmungen betreffend die Risikomanagement- und Sicherheitsmassnahmen sowie der Berichtspflichten durch die wesentliche oder wichtige Einrichtung verstossen wird und dies trotz mehrmaliger Aufforderung der Stabsstelle Cyber-Sicherheit gemäss Art. 15 Abs. 1 Bst. b den rechtmässigen Zustand herzustellen. Für den zu bestimmenden Zeitraum und die Aufgaben des Überwachungsbeauftragten ist die der Benennung zugrunde liegende Begründung ausschlaggebend. In regelmässigen Abständen, jedoch spätestens alle drei Monate hat die Stabsstelle Cyber-Sicherheit zu prüfen, ob die Gründe für die Benennung eines Überwachungsbeauftragten weggefallen sind. Die Begründung, der Zeitraum sowie die festgelegten Aufgaben sowie allfällige Anforderungen an den Überwachungsbeauftragten hat die Stabsstelle Cyber-Sicherheit rechtsmittelfähig zu verfügen. Allfällige Kosten für den Überwachungsbeauftragten sind von der wesentlichen oder wichtigen Einrichtung zu tragen.

Damit wird Art. 32 Abs. 4 Bst. g der Richtlinie (EU) 2022/2555 national umgesetzt.

Die Stabsstelle Cyber-Sicherheit kann gemäss **Abs. 6** wesentliche Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäss Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in Art. 5 genannter Anforderungen nachzuweisen. Mit dieser Bestimmung wird Art. 24 Abs. 1 der Richtlinie (EU) 2022/2555 national umgesetzt.

Abs. 7 befugt die Stabsstelle Cyber-Sicherheit, Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit und in der Regel in Abstimmung mit der betreffenden Einrichtung, durchzuführen. Diese Sicherheitsscans kann der Stabsstelle Cyber-Sicherheit beispielsweise helfen zu überprüfen, ob eine Einrichtung bestimmte Cybersicherheitsmassnahmen implementiert hat. Die Stabsstelle kann für Sicherheitsscans, -prüfungen und Penetrationstests als Reaktion auf Sicherheitsvorfälle auch qualifizierte Dritte nutzen.

Abs. 8 entspricht unverändert Art. 14 Abs. 2 CSG. Die Offenlegung von Informationen gegenüber der Stabsstelle Cyber-Sicherheit betreffend die Sicherheit der Netz- und Informationssysteme, einschliesslich der dokumentierten Sicherheitsmassnahmen oder auch technische und statistische Daten gemäss Abs. 1 Bst. c können gemäss Abs. 8 von Einrichtungen nicht wegen Berufs-, Geschäfts- oder Betriebsgeheimnissen verweigert werden.

Zu Art. 15 – Befugnisse bei Verstössen

Mit dieser Bestimmung werden die Durchsetzungsbefugnisse bei Verstössen gemäss Richtlinie (EU) 2022/2555 umgesetzt. Sie entsprechen – mit Ausnahme redaktioneller Anpassungen – Art. 16 CSG.

Abs. 1 entspricht – mit Ausnahme von redaktionellen Anpassungen – Art. 16 Abs. 1 CSG und legt fest, dass sofern die Stabsstelle Cyber-Sicherheit Anhaltspunkte dafür hat, dass wesentliche und wichtige Einrichtungen gegen Vorschriften dieses Gesetzes, der dazu erlassenen Verordnungen oder gegen darauf gestützte Entscheidungen oder Verfügungen verstösst, sie der Einrichtung eine angemessene Frist setzt und diese formlos auffordert, eine entsprechende Stellungnahme abzugeben (**Bst. a**) oder aber den geforderten rechtmässigen Zustand herzustellen (**Bst. b**).

Gegenständlich wird unter formlos verstanden, dass die Form der Aufforderung an die jeweilige Einrichtung nicht vorgegeben ist. Es handelt sich dabei um eine legistische Formulierung. Die Aufforderung der Stabsstelle Cyber-Sicherheit wird in der Regel schriftlich erfolgen, enthält eine angemessene Frist und ist begründet. Mit dieser formlosen Aufforderung nach Abs. 1 soll vor allem ein aufwändiges Verfahren vermieden und für beide Seiten, sprich für die wesentliche oder wichtige Einrichtung als auch für die Stabsstelle Cyber-Sicherheit, die Klärung oder Lösung überschaubarer Sachverhalte vereinfacht und beschleunigt werden. Kommt eine wesentliche oder wichtige Einrichtung einer formlosen Aufforderung der Stabsstelle Cyber-Sicherheit nicht nach, kann die Stabsstelle eine entsprechende rechtsmittelfähige Verfügung gemäss Abs. 5 erlassen.

Ebenso entsprechen die **Abs. 2 bis 6** mit Ausnahme redaktioneller Anpassungen den Bestimmungen Art. 16 Abs. 2 bis 6 CSG.

Zu Art. 16 – Betrieb von Informations- und Kommunikationstechnik-Lösungen

Die ersten zwei Buchstaben (**Bst. a und b**) entsprechen Art. 17 Bst. a und b CSG.

Zur Erfüllung ihrer Aufgaben ist die Stabsstelle Cyber-Sicherheit berechtigt, gemäss **Bst. c** IKT-Lösungen einzusetzen, um Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter

Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit den wesentlichen oder wichtigen Einrichtungen durchzuführen. Damit wird Art. 32 Abs. 2 Bst. d und Art. 33 Abs. 2 Bst. c der Richtlinie (EU) 2022/2555 umgesetzt. Sicherheitsscans aus der Ferne sind auch Instrument der Aufsicht und können dazu dienen, den Aufwand und die Beeinträchtigung bei der zu kontrollierenden Einrichtung so gering wie möglich zu halten.

Mit **Bst. d** erhält die Stabsstelle Cyber-Sicherheit die Möglichkeit, IKT-Lösungen zu betreiben oder durch Dritte betreiben zu lassen, um Recherchen im Internet, einschliesslich dem sogenannten Darknet, durchzuführen. Dabei ist die Stabsstelle auch befugt, sich in Foren oder auch Internetseiten mit einem geschlossenen Benutzerkreis zu registrieren und anzumelden sowie in weiterer Folge Daten, einschliesslich personenbezogener Daten, aus dem Internet herunterzuladen und zu analysieren. Gerade im Darknet und in geschlossenen Internet-Foren werden regelmässig Zugangsdaten von Unternehmen publiziert und getauscht oder Daten nach einem Ransomware-Angriff veröffentlicht. Eine Analyse derartiger im Internet frei und kostenlos erhältlicher Informationen und Daten kann wichtige Erkenntnisse bringen, die unmittelbar zum Schutz von wesentlichen und wichtigen Einrichtungen eingesetzt werden können.

Zu Art. 17 – Kontrolle

Diese Bestimmung bleibt unverändert und entspricht Art. 18 CSG.

C. Computer-Notfallteam (CSIRT)

Zu Art. 18 – Zweck und Aufgaben

Mit Art. 18 wird Art. 10 bis 12 der Richtlinie (EU) 2022/2555 national umgesetzt und entspricht inhaltlich im Wesentlichen Art. 19 CSG.

Das Computer-Notfallteam (CSIRT) zur Gewährleistung der Cybersicherheit wird gemäss **Abs. 1** bei der Stabsstelle Cyber-Sicherheit eingerichtet. Dem CSIRT kommen insbesondere die in Bst. a bis k aufgeführten Aufgaben zu.

Bst. a bis c entsprechen – mit Ausnahme redaktioneller Anpassungen – Art. 19 Abs. 1 Bst. a bis c CSG und bleiben unverändert.

Neu hinzu kommt die Bereitstellung von Unterstützung für wesentliche und wichtige Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme auf Anfrage (**Bst. d**) sowie auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung auf Schwachstellen mit potenziell signifikanten Auswirkungen oder die proaktive nicht intrusive Überprüfung öffentlich zugänglicher Netz- und Informationssysteme aus eigenem Antrieb (Schwachstellenscan) (**Bst. e**).

Um Sicherheitsvorfällen vorzubeugen, beschäftigt sich das CSIRT insbesondere mit der Vermeidung von Vorfällen und der Prävention. Es soll durch entsprechende Kapazitäten beim CSIRT und/oder über Vereinbarungen mit qualifizierten Dritten sichergestellt werden, dass das CSIRT in der Lage ist, auf Anfrage oder Ersuchen einer wesentlichen oder wichtigen Einrichtung die mit dem Internet verbundenen Anlagen innerhalb und ausserhalb der Geschäftsräume zu überwachen, um das organisatorische Gesamtrisiko der Einrichtung für neu ermittelte Sicherheitslücken in der Lieferkette oder kritische Schwachstellen zu ermitteln, zu verstehen und zu verwalten. Die Anfragen nach Bst. d und Ersuchen nach Bst. e sind von der wesentlichen oder wichtigen Einrichtung zu begründen und dabei ist darzulegen, welche konkreten Massnahmen zur Überwachung bzw. zur Überprüfung ihrer Netz- und Informationssysteme durch die Einrichtung selbst bereits getroffen wurden.

Bst. f bestimmt, dass die Beobachtung und Analyse, einschliesslich die Analyse forensischer Daten sowie die dynamische Analyse, von Risiken und Cyberbedrohungen, Schwachstellen, Sicherheitsvorfällen sowie die Lagebeurteilung, ebenfalls eine Aufgabe des CSIRT ist. Diese Bestimmung entspricht im Wesentlichen Art. 19 Abs. 1 Bst. d CSG, wurde jedoch in Übereinstimmung mit der Richtlinie (EU) 2022/2555 erweitert.

Eine weitere Aufgabe des CSIRTs ist die Zusammenarbeit mit sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen sowie der Austausch von einschlägigen Informationen (**Bst. g**).

Gemäss **Bst. h** obliegen dem CSIRT bei der Stabsstelle Cyber-Sicherheit die Förderung der Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für Verfahren zur Bewältigung von Sicherheitsvorfällen, das Krisenmanagement und die koordinierte Offenlegung von Schwachstellen. Mit dieser Aufgabe wird Art. 11 Abs. 5 der Richtlinie (EU) 2022/2555 umgesetzt.

Bst. i, sprich die Beteiligung am CSIRTs-Netzwerk, entspricht Art. 19 Abs. 1 Bst. e CSG und bleibt unverändert.

Im Zusammenhang mit der Cybersicherheit stellt die internationale Zusammenarbeit ein zentrales Element dar. Das CSIRT vernetzt sich aus diesem Grund international und arbeitet mit nationalen Computer-Notfallteams von Drittländern – hier insbesondere mit der Schweiz – oder gleichwertigen Stellen von Drittländern, insbesondere um Unterstützung im Bereich der Cybersicherheit zu leisten, zusammen und tauscht sich mit diesen aus (**Bst. k**).

Mit **Abs. 2** wird der Stabsstelle Cyber-Sicherheit die Möglichkeit eröffnet, ebenso sonstigen Einrichtungen oder Personen entsprechende Dienstleistungen des CSIRT zukommen zu lassen, sofern diese Einrichtungen oder Personen von einem

Risiko oder einem Sicherheitsvorfall ihrer Netz- und Informationssysteme betroffen sind. Abs. 2 entspricht Art. 19 Abs. 2 CSG.

Als weitere zusätzliche Aufgabe des CSIRT kommt hinzu, dass es zukünftig als Koordinator und vertrauenswürdiger Vermittler zwischen den meldenden natürlichen oder juristischen Personen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten, die wahrscheinlich von der Schwachstelle betroffen sind, für die Zwecke einer koordinierten Offenlegung von Schwachstellen gemäss Art. 12 Abs. 1 der Richtlinie (EU) 2022/2555 fungiert (**Abs. 3**). Zu dieser Aufgabe gehört insbesondere, die betreffenden Einrichtungen zu ermitteln und zu kontaktieren sowie die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen und die Zeitpläne für die Offenlegung auszuhandeln. Ebenso koordiniert das CSIRT das Vorgehen bei Schwachstellen, die mehrere Einrichtungen betreffen. Zur Aufgabenerfüllung kann das CSIRT gemäss Art. 9 Abs. 2 qualifizierte Dritte beiziehen.

Das Nähere über den Zweck und die Aufgaben des CSIRT kann die Regierung mittels Verordnung regeln (**Abs. 4**). Abs. 4 entspricht Art. 19 Abs. 3 CSG.

D. Nationale Cybersicherheitsstrategie

Zu Art. 19 – Grundsatz

Mit Art. 19 wird Art. 7 der Richtlinie (EU) 2022/2555 umgesetzt und entspricht im Wesentlichen Art. 20 CSG. Die Bestimmung sieht vor, dass zwecks Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus, jeder EWR-Mitgliedstaat über eine nationale Strategie (NIS-Strategie) verfügt, in der insbesondere die strategischen Ziele formuliert wurden (**Abs. 1**).

Die Stabsstelle Cyber-Sicherheit wird die besonderen Cybersicherheitsbedürfnisse von kleinen und mittleren Unternehmen bei der Strategieentwicklung einbringen. Kleine und mittlere Unternehmen haben insbesondere damit zu kämpfen, sich an

ein neues Geschäftsgebaren in einer stärker vernetzten Welt anzupassen und sich in der digitalen Umgebung zurechtzufinden. Einige kleine und mittlere Unternehmen stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Cyberbewusstsein, fehlende IT-Sicherheit aus der Ferne, hohe Kosten für Cybersicherheitslösungen und ein erhöhtes Mass an Bedrohungen, wie z. B. Ransomware. Kleine und mittlere Unternehmen werden aufgrund ihrer weniger strengen Risikomanagementmassnahmen im Bereich der Cybersicherheit und ihres geringer ausgeprägten Angriffsmanagements sowie der Tatsache, dass sie über eingeschränkte Sicherheitsressourcen verfügen, zunehmend zum Ziel von Angriffen auf die Lieferkette. Diese Angriffe auf die Lieferkette wirken sich nicht nur auf kleine und mittlere Unternehmen und deren eigene Geschäftstätigkeit aus, sondern können im Rahmen grösserer Angriffe auch eine Kaskadenwirkung auf die von ihnen belieferten Einrichtungen haben.

Abs. 2 legt fest, dass die NIS-Strategie regelmässig, mindestens jedoch alle fünf Jahre, auf der Grundlage wesentlicher Leistungsindikatoren bewertet und falls erforderlich aktualisiert wird. Mit dieser Regelung wird Art. 7 Abs. 4 der Richtlinie (EU) 2022/2555 umgesetzt.

Die Stabsstelle Cyber-Sicherheit zeichnet sich gemäss Art. 13 Abs. 1 Bst. p für die Koordination der Erstellung dieser nationalen Strategie verantwortlich, wobei die Regierung gemäss **Abs. 3** die NIS-Strategie abschliessend genehmigt. Sie wird nach der Genehmigung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht.

IV. Rechtsmittel

Das Kapitel IV. regelt das Rechtsmittel der Beschwerde.

Zu Art. 20 – Beschwerde

Art. 20 entspricht Art. 21 CSG und wurde unverändert übernommen.

V. Strafbestimmungen

Zu Art. 21 – Verwaltungsübertretungen

Mit Art. 21 wird Art. 34 der Richtlinie (EU) 2022/2555 umgesetzt und entspricht im Kern Art. 22 CSG. Es soll mit dieser Bestimmung sichergestellt werden, dass die Geldbussen, die gemäss dem vorliegenden Artikel gegen wesentliche und wichtige Einrichtungen in Bezug auf Verstösse gegen diese Vorlage verhängt werden können, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismässig und abschreckend sind.

Abs. 1 führt Art. 58 Abs. 8 in Verbindung mit Art. 65 der Verordnung (EU) 2019/881 durch. Verstösst eine Einrichtung gegen die Vorschriften der genannten Verordnung, insbesondere gegen die europäischen Schemata für die Cybersicherheitszertifizierung, so kann wegen Übertretung eine Busse bis zu 100 000 Franken verhängt werden. Damit wird der Anforderung nach wirksamen, verhältnismässigen und abschreckenden Sanktionen Rechnung getragen.

Abs. 2 enthält Vorschriften über Sanktionen für Verstösse gegen die nach diesem Gesetz erlassenen Bestimmungen für wesentliche und wichtige Einrichtungen.

Abs. 3 legt fest, dass von der Stabsstelle Cyber-Sicherheit wesentliche Einrichtungen, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, wegen Verstössen nach Abs. 1 mit Busse bis zu 10 000 000 Franken oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist, bestraft werden können. Mit dieser Bestimmung wird Art. 34 Abs. 4 der Richtlinie (EU) 2022/2555 umgesetzt.

Abs. 4 regelt analog der wesentlichen Einrichtungen nach Abs. 3 den Höchstbetrag der Busse für wichtige Einrichtungen. Mit dieser Bestimmung wird Art. 34 Abs. 5 der Richtlinie (EU) 2022/2555 umgesetzt.

Abs. 5 zeigt auf, welche Elemente sowohl bei der Entscheidung über die Verhängung einer Geldbusse sowie auch deren Höhe in jedem Einzelfall durch die Stabsstelle Cyber-Sicherheit zu berücksichtigen sind. Die Elemente entsprechen jenen in Art. 32 Abs. 7 der Richtlinie (EU) 2022/2555.

Falls Verstösse gegen Vorschriften dieses Gesetzes festgestellt werden, wird die Stabsstelle Cyber-Sicherheit gemäss Art. 15 Abs. 1 dies der betreffenden Stelle in einem ersten Schritt formlos mitteilen, und der wesentlichen oder wichtigen Einrichtung eine angemessene Frist setzen, um Stellung zu nehmen oder bestenfalls zeitnah den rechtmässigen Zustand herzustellen. Nur in dringenden Fällen wird die Stabsstelle Cyber-Sicherheit gemäss Art. 15 Abs. 5 ohne Aufforderung eine Verfügung übermitteln und allenfalls eine Busse nach Art. 21 i.V.m. Art. 15 Abs. 6 aussprechen. In Bezug auf die formlose Mitteilung bzw. Aufforderung gemäss Art. 15 Abs. 1 wird auf die dortigen Ausführungen verwiesen.

Abs. 6 nimmt Einrichtungen der öffentlichen Verwaltung von Bussen aus. Mit dieser Bestimmung wird Art. 34 Abs. 7 der Richtlinie (EU) 2022/2555 umgesetzt, wonach unbeschadet der Befugnisse der Stabsstelle Cyber-Sicherheit gemäss Art. 14 und 15 geregelt werden kann, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung Geldbussen verhängt werden können.

Diese Ausnahme rechtfertigt sich dadurch, dass eine dem Staat zufallende Busse vom Staat bezahlt würde. Es fände also lediglich eine interne Umbuchung statt, was nicht sinnvoll erscheint. Trotzdem entsteht durch diese Ausnahme kein sanktionsfreier Raum. Es ist auf das gut ausgebaute Disziplinarrecht, das

bestehende Strafrecht des 22. Abschnitts des Strafgesetzbuches über strafbare Verletzungen der Amtspflicht, Korruption und verwandte strafbare Handlungen zu verweisen.

Die Ausnahme beschränkt sich unter anderem auf Einrichtungen der öffentlichen Verwaltung, welche Teil der Liechtensteinischen Landesverwaltung sind.

Abs. 7 legt fest, dass die Strafobergrenze bei fahrlässiger Begehung auf die Hälfte herabgesetzt wird.

Zu Art. 22 – Verantwortlichkeit

Art. 22 entspricht Art. 23 CSG und wurde unverändert übernommen.

Zu Art. 23 – Besondere Verantwortlichkeit

Mit der Umsetzung der Richtlinie (EU) 2022/2555 ergibt sich eine ergänzende besondere Verantwortlichkeit für Leitungsorgane wesentlicher und wichtiger Einrichtungen, die in der Richtlinie (EU) 2016/1148 und somit im Cyber-Sicherheitsgesetz bisher nicht geregelt sind.

Mit **Abs. 1** wird festgelegt, dass Leitungsorgane wesentlicher und wichtiger Einrichtungen verpflichtet sind, die von diesen Einrichtungen zur Einhaltung von Art. 4 und 5 ergriffenen Risikomanagement- und Sicherheitsmassnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Mit dieser Bestimmung wird Art. 20 Abs. 1 der Richtlinie (EU) 2022/2555 umgesetzt.

Mit **Abs. 2** werden Leitungsorgane wesentlicher und wichtiger Einrichtungen verpflichtet, selbst an Schulungen teilzunehmen und allen Mitarbeitenden 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. Die Nutzung dieser

Angebote sollte auch entsprechend gefördert und seitens der Leitungsorgane unterstützt werden. Mit diesem Absatz wird Art. 20 Abs. 2 der Richtlinie (EU) 2022/2555 umgesetzt.

Mit **Abs. 3** wird geregelt, 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 die Bestimmungen dieses Gesetzes erfüllt.

Die Anwendung der zuvor genannten Bestimmungen lassen andere nationale Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt (**Abs. 4**). Mit dieser Bestimmung wird Art. 20 Abs. 1 Unterabsatz 1 der Richtlinie (EU) 2022/2555 Rechnung getragen.

VI. Schlussbestimmungen

Zu Art. 24 – Durchführungsverordnungen

Diese Bestimmung entspricht Art. 24 CSG und bleibt unverändert.

Zu Art. 25 – Aufhebung bisherigen Rechts

Mit dem Inkrafttreten der gegenständlichen Vorlage wird das Cyber-Sicherheitsgesetz aufgehoben.

Zu Art. 26 – Inkrafttreten

Mit **Abs. 1** wird festgelegt, dass die gegenständliche Revision des Cyber-Sicherheitsgesetzes gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Richtlinie (EU) 2022/2555 in das EWR-

Abkommen in Kraft treten soll. Selbiges gilt für die Verordnung (EU) 2019/881 gemäss **Abs. 2**.

Zu Anhang 1

Anhang 1 entspricht dem Anhang I (Sektoren mit hoher Kritikalität) der Richtlinie (EU) 2022/2555.

Zu Anhang 2

Anhang 2 entspricht dem Anhang II (sonstige kritische Sektoren) der Richtlinie (EU) 2022/2555.

Zu **Anhang 2 Ziff. 1** wird ausgeführt, dass Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG, einschliesslich Anbieter von Kurierdiensten, lediglich dann in den Anwendungsbereich dieses Gesetzes fallen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung, Transport oder Zustellung von Postsendungen, einschliesslich Abholung durch den Empfänger, anbieten. Dabei ist das Ausmass ihrer Abhängigkeit von Netz- und Informationssystemen zu berücksichtigen. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, fallen nicht unter Postdienste.

Zu **Anhang 2 Ziff. 4** bezieht sich auf die Art. 3 Punkt 2 der Verordnung (EG) Nr. 178/2002, in dem ein Lebensmittelunternehmen definiert sind als «Unternehmen, gleichgültig, ob sie auf Gewinnerzielung ausgerichtet sind oder nicht und ob sie öffentlich oder privat sind, die eine mit der Produktion, der Verarbeitung und dem Vertrieb von Lebensmitteln zusammenhängende Tätigkeit ausführen;». Wobei diese Definition für die Zwecke der gegenständlichen Vorlage auf Unternehmen beschränkt wird, die «im Grosshandel sowie in der industriellen Produktion und Verarbeitung tätig sind». Mit dieser Klarstellung in Anhang 2 Ziff. 4 soll die weit gefasste Definition des Begriffs Lebensmittelunternehmen in der Verordnung (EG) Nr. 178/2002 eingeschränkt werden. Durch die Konzentration auf den

Grosshandelsvertrieb wird der Einzelhandel aus dem Anwendungsbereich herausgenommen. In ähnlicher Weise zielen die industrielle Produktion und Verarbeitung darauf ab, den Anwendungsbereich auf die Herstellung und Verarbeitung von Lebensmitteln in grösserem Massstab zu beschränken.

5. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Die gegenständliche Gesetzesvorlage wirft keine verfassungsrechtlichen Fragen auf.

6. AUSWIRKUNGEN AUF DIE NACHHALTIGE ENTWICKLUNG

Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Die Sicherstellung ihrer Verlässlichkeit und Sicherheit ist deshalb von grosser Bedeutung und mit entsprechenden Risikomanagement- und Sicherheitsmassnahmen soll ein hohes, dem Risiko angemessenes Sicherheitsniveau von Netz- und Informationssystemen erreicht werden.

Es wird erwartet, dass die gegenständliche Vorlage Auswirkungen auf die folgenden UNO-Nachhaltigkeitsziele (SDGs) haben wird:

Betroffenes Ziel	**Relevante Unterziele**	**Zu erwartende Auswirkungen durch die Regierungsvorlage**
SDG 5 Geschlechtergleichheit	5.b, 5.1, 5.5	Funktionierende und cybersichere Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Die Sicherstellung ihrer Verlässlichkeit und

		Sicherheit ist auch wesentlicher Baustein für die Nutzung von Grundlagentechnologien, insbesondere der Informations- und Kommunikationstechnologien, um die Selbstbestimmung der Frauen zu fördern. Auch bei der Erstellung der nationalen Strategie von Netz- und Informationssystemen wird der Gender Dimension Rechnung getragen: Zum einen durch die Zusammensetzung der Personen/Arbeitsgruppe, die mit der Erarbeitung der Strategie betraut werden, und zum anderen dadurch, dass diese Dimension bei der inhaltlichen Erarbeitung der Strategie berücksichtigt wird. Ebenso wird das Thema bei der Sensibilisierung gem. Art. 13 Abs. 1 Bst. k entsprechend berücksichtigt. Zudem soll durch ein Angebot von Ausbildung und Training die volle und wirksame Teilhabe von Frauen und ihre Chancengleichheit bei der Übernahme von Führungsrollen auf allen Ebenen der Entscheidungsfindung sichergestellt werden.

SDG 6 Sauberes Wasser und Sanitäreinrichtungen	6.3, 6.4, 6.5, 6.6	Wasserbewirtschaftung zählt zur kritischen Infrastruktur und ist besonders zu schützen. Durch externe Einflüsse, insbesondere Sicherheitsvorfälle kann diese gefährdet werden. Die vorgesehenen Massnahmen dienen auch dem Schutz der angeführten Ziele.
SDG 8 Menschenwürdige Arbeit und Wirtschaftswachstum	8.2, 8.3	Hohe Cybersicherheits-Standards, technologische Modernisierung und Innovation sind notwendig für das Wachstum von Kleinst-, Klein- und Mittelunternehmen.
SDG 9 Industrie, Innovation und Infrastruktur	9.1, 9.4	Zu einer hochwertigen, verlässlichen, nachhaltigen und widerstandsfähigen Infrastruktur verpflichten, Infrastrukturen modernisieren um sie widerstandsfähig gegenüber Cyberangriffen und damit nachhaltig auszurichten. Anreize setzen für Marktteilnehmer, die Infrastruktur zu modernisieren, um sie nachhaltig zu machen, mit effizienterem Ressourceneinsatz.
SDG 16 Frieden, Gerechtigkeit und starke Institutionen	16.6, 16.10	Sichere Netz- und Informationssysteme spielen eine zentrale Rolle für das Funktionieren des staatlichen Gemeinwesens. Dies betrifft auch den

		Schutz der Rechtsstaatlichkeit, Sicherung leistungsfähiger Institutionen, Schutz der Grundfreiheite n, insbesondere durch Schutz des öffentlichen Zugangs zu Informationen.

Die Regierung geht davon aus, dass sich die Umsetzung des Vorhabens insgesamt auf 13 SDGs positiv auswirken wird. Gleichzeitig wird nicht mit negativen Auswirkungen auf die SDGs gerechnet. Die Regierung kommt deshalb zum Schluss, dass die Vorlage die Nachhaltigkeit im Sinne der SDGs verbessert.

7. REGIERUNGSVORLAGE

Cyber-Sicherheitsgesetzes (CSG)

vom ...

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

I. Allgemeine Bestimmungen

Art. 1

Gegenstand und Geltungsbereich

1) Dieses Gesetz legt die Massnahmen fest, mit denen ein hohes Cybersicherheitsniveau erreicht werden soll von öffentlichen und privaten Einrichtungen der im Anhang 1 und 2 genannten Art, die nach Art. 1064 Abs. 2 oder Abs. 3 PGR als mittelgrosse oder grosse Gesellschaften gelten und ihre Dienste im EWR erbringen oder ihre Tätigkeiten dort ausüben.

2) Unabhängig von der Grösse der Einrichtungen gilt dieses Gesetz auch für Einrichtungen der im Anhang 1 und 2 genannten Art, wenn

a) die Dienste erbracht werden von:

1. Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;

2. Vertrauensdiensteanbietern;

3. TLD-Namenregistern und DNS-Diensteanbietern;

b) es sich bei der Einrichtung um den einzigen Anbieter handelt, der einen Dienst erbringt, 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 EWR-Mitgliedstaat hat, kritisch ist; oder

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung ist.

3) Unabhängig von der Grösse der Einrichtungen gilt dieses Gesetz ebenso für Einrichtungen,

a) die nach der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden;

b) die Domänennamenregistrierungsdienste erbringen.

4) Die in diesem Gesetz vorgesehenen Risikomanagementmassnahmen und Berichtspflichten gemäss Art. 4 und 6 gelten nicht für:

a) 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;

b) Einrichtungen, die gemäss Art. 2 Abs. 4 der Verordnung (EU) 2022/2554 vom Anwendungsbereich dieser Verordnung ausgenommen sind.

Art. 2

Umsetzung und Durchführung von EWR-Rechtsvorschriften

1) Dieses Gesetz dient der Umsetzung bzw. Durchführung folgender EWR-Rechtsvorschriften:

a) Richtlinie (EU) 2022/2555 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie)[4];

b) Verordnung (EU) 2021/887 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren[5];

c) Verordnung (EU) 2019/881 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik[6].

---

[4] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Massnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80)

[5] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (ABl. L 202 vom 8.6.2021, S. 1)

[6] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15)

2) Die gültige Fassung der EWR-Rechtsvorschriften, auf die in diesem Gesetz Bezug genommen wird, ergibt sich aus der Kundmachung der Beschlüsse des Gemeinsamen EWR-Ausschusses im Liechtensteinischen Landesgesetzblatt nach Art. 3 Bst. k des Kundmachungsgesetzes.

Art. 3

Begriffsbestimmungen und Bezeichnungen

1) Im Sinne dieses Gesetzes gelten als:

1. "Netz- und Informationssystem":

   a) ein elektronisches Kommunikationsnetz im Sinne von Art. 3 Abs. 1 Ziff. 13 des Kommunikationsgesetzes;

   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 Bst. 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": bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;

4. "NIS-Strategie" (Nationale Cybersicherheitsstrategie): ein kohärenter Rahmen mit strategischen Zielen und Prioritäten im Bereich der Cybersicherheit und der zu ihrer Verwirklichung erforderlichen Governance;

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

6. "Sicherheitsvorfall": jedes Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder entsprechender Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigen;

7. "erheblicher Sicherheitsvorfall": ein Sicherheitsvorfall, wenn er

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

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

8. "Cybersicherheitsvorfall grossen Ausmasses": ein Sicherheitsvorfall, der eine Störung verursacht, deren Ausmass die Reaktionsfähigkeit eines EWR-

Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei EWR-Mitgliedstaaten hat;

9. "Bewältigung von Sicherheitsvorfällen": alle Massnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon;

10. "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;

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

12. "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;

13. "IKT-Produkt": ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;

14. "IKT-Dienst": ein Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;

15. "IKT-Prozess" jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;

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

17. "Norm": eine Norm im Sinne des Art. 2 Ziff. 1 der Verordnung (EU) Nr. 1025/2012[7];

18. "technische Spezifikation" eine technische Spezifikation im Sinne des Art. 2 Ziff. 4 der Verordnung (EU) Nr. 1025/2012;

19. "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;

20. "Domänennamensystem (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;

21. "DNS-Diensteanbieter": eine Einrichtung, die

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

---

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

22. "Namenregister der Domäne der ersten Ebene" oder "TLD-Namenregister": eine Einrichtung, der eine bestimmte Domäne der ersten Ebene (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;

23. "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;

24. "digitaler Dienst": ein Dienst im Sinne des Art. 1 Abs. 1 Bst. b der Richtlinie (EU) 2015/1535[8];

25. "Vertrauensdienst": ein Vertrauensdienst im Sinne des Art. 3 Ziff. 16 der Verordnung (EU) Nr. 910/2014[9];

26. "Vertrauensdiensteanbieter" einen Vertrauensdiensteanbieter im Sinne des Art. 3 Ziff. 19 der Verordnung (EU) Nr. 910/2014;

---

[8] 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 (kodifizierter Text) (ABl. L 241 vom 17.9.2015, S. 1)

[9] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73)

27. "qualifizierter Vertrauensdienst" einen qualifizierten Vertrauensdienst im Sinne des Art. 3 Ziff. 17 der Verordnung (EU) Nr. 910/2014;

28. "qualifizierter Vertrauensdiensteanbieter" einen qualifizierten Vertrauensdiensteanbieter im Sinne des Art. 3 Ziff. 20 der Verordnung (EU) Nr. 910/2014;

29. "Online-Marktplatz": ein Dienst, der es Verbrauchern durch die Verwendung von Software, einschliesslich einer Internetseite, eines Teils einer Internetseite oder einer Anwendung, die vom oder im Namen des Gewerbetreibenden betrieben wird, ermöglicht, Fernabsatzverträge mit anderen Gewerbetreibenden oder Verbrauchern, abzuschliessen;

30. "Online-Suchmaschine": ein digitaler Dienst, der es Nutzern ermöglicht, in Form eines Stichworts, einer Spracheingabe, einer Wortgruppe oder einer anderen Eingabe Anfragen einzugeben, um prinzipiell auf allen Internetseiten oder auf allen Internetseiten in einer bestimmten Sprache eine Suche zu einem beliebigen Thema vorzunehmen und Ergebnisse in einem beliebigen Format angezeigt zu bekommen, über die sie Informationen im Zusammenhang mit dem angeforderten Inhalt finden können;

31. "Cloud-Computing-Dienst": ein digitaler 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;

32. "Rechenzentrumsdienst": ein 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;

33. "Inhaltszustellnetz": 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;

34. "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;

35. "Vertreter": eine im EWR 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 im EWR 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 dieses Gesetzes wenden kann;

36. "öffentliches elektronisches Kommunikationsnetz": ein öffentliches elektronisches Kommunikationsnetz im Sinne von Art. 3 Abs. 1 Ziff. 15 KomG;

37. "elektronischer Kommunikationsdienst": ein elektronischer Kommunikationsdienst im Sinne des Art. 3 Abs. 1 Ziff. 8 KomG;

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": ein 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;

42. "Kooperationsgruppe": ein nach Art. 14 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der EWR-Mitgliedstaaten, der Europäischen Kommission und der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) zusammensetzt und der Unterstützung und Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den EWR-Mitgliedstaaten zum Aufbau von Vertrauen und zur Erreichung eines hohen Cybersicherheitsniveaus im EWR dient;

43. "CSIRTs-Netzwerk": ein nach Art. 15 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der Computer-Notfallteams der EWR-Mitgliedstaaten und des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) zusammensetzt und zum Aufbau von Vertrauen zwischen den EWR-Mitgliedstaaten beitragen sowie eine rasche und wirksame operative Zusammenarbeit fördern soll;

44. "EU-CyCLONe" (European Cyber Crises Liaison Organisation Network): ein nach Art. 16 der Richtlinie (EU) 2022/2555 eingerichtetes Gremium, das sich aus Vertretern der Behörden für das Cyberkrisenmanagement der EWR-Mitgliedstaaten und der Europäischen Kommission zusammensetzt und bei der koordinierten Bewältigung von Cybersicherheitsvorfällen grossen Ausmasses und Krisen auf operativer Ebene sowie bei der Gewährleistung eines regelmässigen Austauschs relevanter Informationen zwischen den EWR-Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen unterstützen soll.

2) Im Sinne dieses Gesetzes gelten als wesentliche Einrichtungen:

a) Einrichtungen der in Anhang 1 aufgeführten Art, die die in Art. 1064 Abs. 2 PGR genannten Schwellenwerte für mittelgrosse Gesellschaften überschreiten;

b) qualifizierte Vertrauensdiensteanbieter und TLD-Namenregister sowie DNS-Diensteanbieter, unabhängig von ihrer Grösse;

c) Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Art. 1064 Abs. 2 PGR als mittelgrosse Gesellschaften gelten;

d) Einrichtungen der öffentlichen Verwaltung;

e) sonstige Einrichtungen der in Anhang 1 oder 2 aufgeführten Art, die von der Regierung mit Verordnung gemäss Art. 1 Abs. 2 Bst. b bis e als wesentliche Einrichtungen eingestuft werden;

f) Einrichtungen, die gemäss der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden.

3) Im Sinne dieses Gesetzes gelten als wichtige Einrichtungen:

a) Einrichtungen der in Anhang 1 oder 2 aufgeführten Art, die nicht als wesentliche Einrichtungen im Sinne von Abs. 2 gelten;

b) sonstige Einrichtungen der in Anhang 1 oder 2 aufgeführten Art, die von der Regierung mit Verordnung gemäss Art. 1 Abs. 2 Bst. b bis e als wichtige Einrichtungen eingestuft wurden.

4) Unter den in diesem Gesetz verwendeten Personenbezeichnungen sind alle Personen unabhängig ihres Geschlechts zu verstehen, sofern sich die Personenbezeichnungen nicht ausdrücklich auf ein bestimmtes Geschlecht beziehen.

II. Risikomanagementmassnahmen und Berichtspflichten

A. Wesentliche und wichtige Einrichtungen

Art. 4

Risikomanagementmassnahmen

Wesentliche und wichtige Einrichtungen ergreifen geeignete und verhältnismässige technische, operative und organisatorische Massnahmen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie 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.

Art. 5

Sicherheitsmassnahmen

1) Die Massnahmen nach Art. 4 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, welches 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 Massnahmen nach Art. 4 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;

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

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

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

3) Die Einrichtungen berücksichtigen bei der Erwägung geeigneter Massnahmen nach Abs. 2 Bst. d bei den einzelnen unmittelbaren Anbietern und Diensteanbietern:

a) die spezifischen Schwachstellen;

b) die Gesamtqualität der Produkte;

c) die Cybersicherheitspraxis;

d) die Sicherheit der Entwicklungsprozesse.

4) Stellt eine Einrichtung fest, dass sie den Massnahmen nach Abs. 2 nicht nachkommt, ergreift sie unverzüglich alle erforderlichen, angemessenen und verhältnismässigen Korrekturmassnahmen.

5) Die Pflichten nach Abs. 1 bis 4 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über Risikomanagementmassnahmen bestehen, die zumindest ein gleichwertiges Cybersicherheitsniveau vorsehen.

6) Die Regierung kann das Nähere über die Sicherheitsmassnahmen mit Verordnung regeln.

Art. 6

Berichtspflichten

1) Wesentliche und wichtige Einrichtungen haben erhebliche Sicherheitsvorfälle der Stabsstelle Cyber-Sicherheit zu melden und dabei Folgendes zu 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) unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die unter Bst. a genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschliesslich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

2) Auf Ersuchen der Stabsstelle Cyber-Sicherheit übermittelt die von einem erheblichen Sicherheitsvorfall betroffene Einrichtung der Stabsstelle Cyber-Sicherheit einen Zwischenbericht über relevante Statusaktualisierungen.

3) Spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls nach Abs. 1 Bst. b hat die betroffene Einrichtung der Stabsstelle Cyber-Sicherheit einen Fortschrittsbericht im Falle eines andauernden Sicherheitsvorfalls oder einen Abschlussbericht nach Abschluss der Behandlung des Sicherheitsvorfalls zu übermitteln.

4) Der Abschlussbericht nach Abs. 3 hat zumindest Folgendes zu enthalten:

a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschliesslich seines Schweregrads und seiner Auswirkungen;

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

c) Angaben zu den getroffenen und laufenden Abhilfemassnahmen;

d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

5) Wesentliche und wichtige Einrichtungen informieren gegebenenfalls jene Empfänger ihrer Dienste unverzüglich über den erheblichen Sicherheitsvorfall, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Gegebenenfalls teilen die wesentlichen und wichtigen Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich Massnahmen oder Abhilfemassnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können.

6) Meldungen sind in einem gesicherten und soweit möglich standardisierten elektronischen Format zu übermitteln.

7) Die Pflichten nach Abs. 1 bis 5 finden keine Anwendung, wenn spezialgesetzliche Bestimmungen über eine Meldepflicht bestehen und die Kriterien für diese Meldepflicht mindestens gleichwertig sind. In diesen Fällen haben die Meldungsempfänger die bei ihnen eingegangenen Meldungen unverzüglich an die Stabsstelle Cyber-Sicherheit weiterzuleiten.

8) Die Regierung kann das Nähere über die Berichtspflicht für wesentliche und wichtige Einrichtungen mit Verordnung regeln.

Art. 7

Information der Öffentlichkeit

Nach einer Meldung gemäss Art. 6 Abs. 1 Bst. b und Anhörung der betreffenden Einrichtung kann die Stabsstelle Cyber-Sicherheit die Öffentlichkeit über konkrete Sicherheitsvorfälle informieren oder verlangen, dass die Einrichtung dies unternimmt, wenn:

a) die Sensibilisierung der Öffentlichkeit zur Verhütung von Sicherheitsvorfällen oder zur Bewältigung aktueller Sicherheitsvorfälle erforderlich ist; oder

b) die Offenlegung des Sicherheitsvorfalls auf sonstige Weise im öffentlichen Interesse liegt.

B. Andere Einrichtungen

Art. 8

Freiwillige Meldung

1) Jede Einrichtung kann Sicherheitsvorfälle, Cyberbedrohungen oder Beinahe-Vorfälle der Stabsstelle Cyber-Sicherheit melden.

2) Die freiwillige Meldung muss weder die Identität der Einrichtung noch Informationen, die auf diese schliessen lassen, enthalten.

III. Organisation und Durchführung

A. Allgemeines

Art. 9

Zuständigkeit

1) Mit der Durchführung dieses Gesetzes sind betraut:

a) die Stabsstelle Cyber-Sicherheit;

b) das Computer-Notfallteam (CSIRT).

2) Die Stabsstelle Cyber-Sicherheit und das CSIRT können zur Erfüllung ihrer Aufgaben qualifizierte Dritte beauftragen.

3) Die Regierung kann das Nähere über die Anforderungen an qualifizierte Dritte nach Abs. 2 mit Verordnung regeln.

Art. 10

Amtsgeheimnis

Die mit der Durchführung dieses Gesetzes betrauten Organe sowie allfällig durch diese beauftragte qualifizierte Dritte unterliegen dem Amtsgeheimnis und haben gegenüber anderen Amtsstellen und Personen über die in Ausübung dieser Tätigkeit gemachten Wahrnehmungen Stillschweigen zu bewahren und Einsicht in verarbeitete Daten und amtliche Akten zu verweigern. Art. 14 bleibt vorbehalten.

Art. 11

Verarbeitung und Offenlegung personenbezogener Daten

1) Die Stabsstelle Cyber-Sicherheit ist berechtigt, zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz die erforderlichen, einschliesslich der besonderen Kategorien, personenbezogenen Daten nach Art. 4 Ziff. 1 bzw. Art. 9 der Verordnung (EU) 2016/679[10], zu verarbeiten.

2) Sie kann Daten nach Abs. 1, die ihr aufgrund der Wahrnehmung ihrer Aufgaben nach diesem Gesetz bekannt sind, in- und ausländischen Behörden und Stellen offenlegen, wenn:

a) dies zur Erfüllung ihrer Aufgaben nach diesem Gesetz oder der Richtlinie (EU) 2022/2555 erforderlich ist;

b) die Vertraulichkeit der Daten gewährleistet ist; sowie

c) die Sicherheit und die geschäftlichen Interessen der wesentlichen und wichtigen Einrichtungen geschützt sind.

[10] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1)

3) Einrichtungen können auf freiwilliger Basis Informationen betreffend die Cybersicherheit untereinander austauschen, insbesondere über:

a) Cyberbedrohungen;

b) Schwachstellen;

c) Taktiken, Techniken und Verfahren;

d) Kompromittierungsindikatoren;

e) Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen;

f) Beinahe-Vorfälle.

4) Der Informationsaustausch nach Abs. 3 dient dem Zweck:

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

b) das Cybersicherheitsniveau zu erhöhen, insbesondere indem

1. Aufklärungsarbeit über Cyberbedrohungen geleistet wird,

2. die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird,

3. Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden, oder

4. die gemeinsame Forschung im Bereich Cyberbedrohung zwischen öffentlichen und privaten Einrichtungen gefördert wird.

B. Stabsstelle Cyber-Sicherheit

Art. 12

Zuständigkeit

1) Die Stabsstelle Cyber-Sicherheit ist die für die Cybersicherheit zuständige nationale Behörde nach Art. 8 Abs. 1 der Richtlinie (EU) 2022/2555. Ihr obliegt die Aufsicht und der Vollzug dieses Gesetzes.

2) Die Stabsstelle Cyber-Sicherheit ist die für die Cybersicherheit zuständige zentrale Anlaufstelle nach Art. 8 Abs. 3 der Richtlinie (EU) 2022/2555. Sie ist die Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit internationalen Gremien und Gruppen, wie insbesondere den zuständigen Stellen in anderen EWR-Mitgliedstaaten, der Kooperationsgruppe und dem CSIRTs-Netzwerk.

3) Die Stabsstelle Cyber-Sicherheit ist die für das Management von Cybersicherheitsvorfällen grossen Ausmasses und Krisen zuständige Behörde nach Art. 9 Abs. 1 der Richtlinie (EU) 2022/2555.

4) Die Stabsstelle Cyber-Sicherheit ist die nationale Behörde für Cybersicherheitszertifizierungen nach Art. 58 Abs. 1 der Verordnung (EU) 2019/881 und nimmt die Aufgaben und Befugnisse nach Art. 58 Abs. 7 und 8 der Verordnung (EU) 2019/881 wahr.

Art. 13

Aufgaben

1) Die Stabsstelle Cyber-Sicherheit trifft die im Rahmen ihrer Zuständigkeit erforderlichen Massnahmen, um die Einhaltung dieses Gesetzes sicherzustellen. Ihr obliegen insbesondere:

a) die Überprüfung der Risikomanagement- und Sicherheitsmassnahmen nach Art. 4 und 5 sowie die Einhaltung der Berichtspflichten nach Art.6;

b) die Einrichtung und Koordination des CSIRT nach Art. 18;

c) die Entgegennahme und Analyse von Meldungen über Risiken oder Sicherheitsvorfälle, die Erstellung eines diesbezüglichen Lagebildes und Weiterleitung der Meldungen sowie des Lagebildes und zusätzlicher relevanter Informationen an inländische Behörden oder andere betroffene Stellen bei Bedarf;

d) die Erstellung und Weitergabe von relevanten Informationen zur Gewährleistung der Cybersicherheit oder zur Vorbeugung von Sicherheitsvorfällen;

e) die Erstellung einer Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sowie die regelmässige, mindestens jedoch einmal alle zwei Jahre, Überprüfung und Aktualisierung dieser Liste;

f) die Entgegennahme von Nennungen und das Führen einer Liste der Vertreter gemäss Art. 3 Abs. 1 Ziff. 35;

g) die Förderung der Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen;

h) die Unterrichtung und Weiterleitung von durch wesentliche und wichtige Einrichtungen bereitgestellten Informationen an die zentrale Anlaufstelle der betroffenen EWR-Mitgliedstaaten, wenn ein Sicherheitsvorfall eine grenzüberschreitende Auswirkung in diesen EWR-Mitgliedsstaaten hat;

i) die Koordination und die Förderung der öffentlich-privaten Zusammenarbeit im Bereich der Cybersicherheit;

k) die Unterrichtung der Öffentlichkeit über Sicherheitsvorfälle, die Sensibilisierung der Öffentlichkeit zur Verhütung oder Bewältigung von Sicherheitsvorfällen sowie die Veröffentlichung allgemeiner Informationen im Zusammenhang mit der Cybersicherheit;

l) die Zusammenarbeit und der Informationsaustausch mit anderen inländischen Behörden und Stellen, insbesondere der Landespolizei, der Staatsanwaltschaft, der Datenschutzstelle, dem Amt für Informatik, dem Amt für Kommunikation, dem Amt für Bevölkerungsschutz, dem Amt für Hochbau und Raumplanung, dem Amt für Tiefbau und Geoinformation, der Stabsstelle FIU und der Finanzmarktaufsicht Liechtenstein;

m) die Zusammenarbeit mit dem Landesführungsstab und die Koordination der Ausarbeitung eines nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle grossen Ausmasses und Krisen;

n) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch, wie etwa im Falle der Amtshilfe oder eines erheblichen Sicherheitsvorfalls oder bei einem Cybersicherheitsvorfall grossen Ausmasses, von dem zwei oder mehr EWR-Mitgliedstaaten betroffen sind, mit den zuständigen Behörden und Stellen in anderen EWR-Mitgliedstaaten, der ENISA, der Kooperationsgruppe, dem EU-CyCLONe und dem CSIRTs-Netzwerk;

o) die grenzüberschreitende Zusammenarbeit und der grenzüberschreitende Informationsaustausch im Bereich der Cybersicherheit mit den zuständigen Behörden und Stellen in Drittstaaten;

p) die Koordination der Erstellung einer NIS-Strategie nach Art. 19;

q) die Vertretung Liechtensteins, in der Kooperationsgruppe, dem CSIRTs-Netzwerk, dem EU-CyCLONe, der Europäischen Gruppe für die Cybersicherheitszertifizierung sowie in anderen grenzüberschreitenden Gremien im EWR und internationalen Gremien für die Cybersicherheit.

r) die Teilnahme an Peer Reviews gemäss Art. 19 der Richtlinie (EU) 2022/2555;

2) Die Stabsstelle Cyber-Sicherheit kann nach Rücksprache mit dem zuständigen Regierungsmitglied mit anderen in- und ausländischen Behörden Vereinbarungen über die Modalitäten der Zusammenarbeit abschliessen sowie zur Aufgabenerfüllung mit Privaten im Rahmen von öffentlich-privaten Partnerschaften zusammenarbeiten.

3) Die Regierung kann das Nähere über die Aufgaben der Stabsstelle Cyber-Sicherheit mit Verordnung regeln.

Art. 14

Befugnisse gegenüber wesentlichen und wichtigen Einrichtungen

1) Die Stabsstelle Cyber-Sicherheit kann bei der Wahrnehmung ihrer Aufgaben nach diesem Gesetz von den wesentlichen und wichtigen Einrichtungen verlangen, dass sie ihr:

a) die zur Bewertung der Cybersicherheit erforderlichen Informationen, einschliesslich der ergriffenen Risikomanagementmassnahmen sowie der dokumentierten Cybersicherheitskonzepte, zur Verfügung stellen;

b) Nachweise für die wirksame Umsetzung der Cybersicherheitskonzepte erbringen;

c) Informationen, insbesondere technische und statistische Daten, zu statistischen Zwecken oder für die Erstellung konkreter Lagebilder unentgeltlich offenlegen.

2) Die Stabsstelle Cyber-Sicherheit kann von wesentlichen und wichtigen Einrichtungen zur Wahrnehmung ihrer Aufgaben nach diesem Gesetz folgende Angaben verlangen:

a) Name der Einrichtung;

b) Sektor, Teilsektor und Art der Einrichtung gemäss Anhang 1 oder 2;

c) Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen im EWR oder, falls sie nicht im EWR niedergelassen ist, Anschrift ihres Vertreters oder Zustellungsbevollmächtigten;

d) aktuelle Kontaktdaten, einschliesslich E-Mail-Adressen und Telefonnummern der Einrichtung und gegebenenfalls ihres Vertreters;

e) die EWR-Mitgliedstaaten, in denen die Einrichtung Dienste erbringt;

f) die IP-Adressbereiche der Einrichtung.

3) Wesentliche und wichtige Einrichtungen übermitteln der Stabsstelle Cyber-Sicherheit zwecks Registrierung unverzüglich, in jedem Fall aber innerhalb von vier Wochen ab Inkrafttreten dieses Gesetzes die Angaben nach Abs. 2. Wesentliche und wichtige Einrichtungen informieren die Stabsstelle Cyber-

Sicherheit unverzüglich über jede Änderung der Angaben nach Abs. 2, in jedem Fall aber innerhalb von zwei Wochen ab dem Tag der Änderung.

4) Die Stabsstelle Cyber-Sicherheit kann wesentliche oder wichtige Einrichtungen anweisen, 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.

5) Die Stabsstelle Cyber-Sicherheit kann wesentliche oder wichtige Einrichtungen in begründeten Fällen verpflichten, für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung der Art. 4 bis 6 durch die betreffenden Einrichtungen überwacht.

6) Die Stabsstelle Cyber-Sicherheit kann wesentliche Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäss Art. 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in Art. 5 genannter Anforderungen nachzuweisen.

7) Die Stabsstelle Cyber-Sicherheit ist befugt, Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung, durchzuführen.

8) Wesentliche und wichtige Einrichtungen können die Offenlegung von Informationen nach Abs. 1 Bst. c nicht wegen Berufs-, Geschäfts- oder Betriebsgeheimnissen verweigern.

Art. 15

Befugnisse bei Verstössen

1) Hat die Stabstelle Cyber-Sicherheit Anhaltspunkte dafür, dass eine wesentliche oder wichtige Einrichtung gegen Vorschriften dieses Gesetzes, der dazu erlassenen Verordnungen oder gegen darauf gestützte Entscheidungen oder Verfügungen verstösst, teilt sie dies der wesentlichen oder wichtigen Einrichtung vorbehaltlich Abs. 5 formlos mit und setzt ihr eine angemessene Frist, um:

a) zur Mitteilung Stellung zu nehmen; oder

b) den rechtmässigen Zustand herzustellen.

2) Die Stabsstelle Cyber-Sicherheit kann die Frist nach Abs. 1 Bst. b in begründeten Fällen auf Antrag angemessen verlängern, wenn die wesentliche oder wichtige Einrichtung dadurch voraussichtlich den rechtmässigen Zustand herstellt.

3) Handelt es sich bei der wesentlichen oder wichtigen Einrichtung um eine öffentliche Stelle oder eine Stelle, welche mit öffentlichen Aufgaben betraut ist, informiert die Stabsstelle Cyber-Sicherheit zusätzlich die Regierung über die Aufforderung nach Abs. 1.

4) Die Stabsstelle Cyber-Sicherheit informiert bei Anhaltspunkten zu Verstössen gegen Vorschriften dieses Gesetzes oder dazu erlassenen Verordnungen durch wesentliche oder wichtige Einrichtungen die zuständige

Aufsichtsbehörde und gibt dieser vor einer Aufforderung nach Abs. 1 Gelegenheit zur Stellungnahme.

5) Kommt eine wesentliche oder wichtige Einrichtung der Aufforderung nach Abs. 1 nicht nach, so erlässt die Stabsstelle Cyber-Sicherheit eine entsprechende Verfügung; in dringenden Fällen kann auch ohne Aufforderung eine Verfügung erfolgen. Die Stabsstelle Cyber-Sicherheit informiert die zuständige Aufsichtsbehörde der wesentlichen oder wichtigen Einrichtung über die Entscheidung.

6) Die Verhängung von Bussen nach Art. 21 bleibt vorbehalten.

Art. 16

Betrieb von Informations- und Kommunikationstechnik-Lösungen (IKT-Lösungen)

Die Stabsstelle Cyber-Sicherheit ist zur Erfüllung ihrer Aufgaben berechtigt:

a) IKT-Lösungen zu betreiben oder durch Dritte betreiben zu lassen, die Risiken oder Sicherheitsvorfälle von Netz- und Informationssystemen frühzeitig erkennen;

b) IKT-Lösungen zu betreiben oder nach Einwilligung der betroffenen Einrichtung zu nutzen, um die Muster von Angriffen auf Netz- und Informationssysteme zu erkennen;

c) IKT-Lösungen einzusetzen, um Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit den wesentlichen oder wichtigen Einrichtungen durchzuführen;

d) IKT-Lösungen zu betreiben oder durch Dritte betreiben zu lassen, um Recherchen im Internet durchzuführen, sich dabei auch an Foren oder

Internetseiten mit einem geschlossenen Benutzerkreis zu registrieren und anzumelden sowie in weiterer Folge Daten, einschliesslich personenbezogener Daten, aus dem Internet herunterzuladen und zu analysieren.

Art. 17

Kontrolle

1) Die Stabsstelle Cyber-Sicherheit kann Kontrollen zur Einhaltung der Anforderungen nach diesem Gesetz durchführen oder durch von ihr beauftragte qualifizierte Dritte durchführen lassen.

2) Zur Durchführung von Kontrollen können die Stabsstelle Cyber-Sicherheit oder von ihr beauftragte qualifizierte Dritte, Einsicht in die Netz- und Informationssysteme, die von wesentlichen und wichtigen Einrichtungen genutzt werden, und diesbezügliche Unterlagen nehmen. Dabei sind sie berechtigt, Örtlichkeiten, in welchen Netz- und Informationssysteme gelegen sind, zu betreten. Die Ausübung der Einsicht hat verhältnismässig zu erfolgen und ist unter möglichster Schonung der Rechte der betroffenen Einrichtung und Dritter sowie des Betriebs auszuüben.

3) Die Regierung kann das Nähere über die Durchführung von Kontrollen mit Verordnung regeln.

C. Computer-Notfallteam (CSIRT)

Art. 18

Zweck und Aufgaben

1) Zur Gewährleistung der Cybersicherheit wird bei der Stabsstelle Cyber-Sicherheit ein CSIRT eingerichtet. Ihm obliegen insbesondere:

a) gegebenenfalls das zur Verfügung stellen von zur Bewältigung eines Sicherheitsvorfalls nützlichen Informationen oder Orientierungshilfen für die Durchführung möglicher Abhilfemassnahmen nach Eingang von Meldungen über Risiken oder Sicherheitsvorfälle nach Art. 6 und 8;

b) die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle unter den einschlägigen Interessensträgern;

c) die erste allgemeine oder technische Unterstützung bei der Reaktion auf einen Sicherheitsvorfall;

d) die Bereitstellung von Unterstützung für wesentliche und wichtige Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme auf Anfrage;

e) auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung auf Schwachstellen mit potenziell signifikanten Auswirkungen oder die proaktive nicht intrusive Überprüfung öffentlich zugänglicher Netz- und Informationssysteme aus eigenem Antrieb (Schwachstellenscan);

f) die Beobachtung und Analyse, einschliesslich die Analyse forensischer Daten sowie die dynamische Analyse, von Risiken und Cyberbedrohungen, Schwachstellen, Sicherheitsvorfällen sowie die Lagebeurteilung;

g) die Zusammenarbeit mit sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen sowie der Austausch von einschlägigen Informationen;

h) die Förderung der Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für Verfahren zur Bewältigung von Sicherheitsvorfällen, das Krisenmanagement und die koordinierte Offenlegung von Schwachstellen;

i) die Beteiligung am CSIRTs-Netzwerk;

k) die Zusammenarbeit mit nationalen Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern, insbesondere um Unterstützung im Bereich der Cybersicherheit zu leisten.

2) Das CSIRT kann die Aufgaben nach Abs. 1 Bst. a bis c auch gegenüber sonstigen Einrichtungen oder Personen wahrnehmen, wenn diese von einem Risiko oder einem Sicherheitsvorfall ihrer Netz- und Informationssysteme betroffen sind.

3) Das CSIRT fungiert als Koordinator und vertrauenswürdiger Vermittler für die Zwecke einer koordinierten Offenlegung von Schwachstellen gemäss Art. 12 Abs. 1 der Richtlinie (EU) 2022/2555.

4) Die Regierung kann das Nähere über den Zweck und die Aufgaben des CSIRT mit Verordnung regeln.

D. Nationale Cybersicherheitsstrategie

Art. 19

Grundsatz

1) Die NIS-Strategie bestimmt insbesondere die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen und die angemessenen Politik- und Regulierungsmassnahmen, mit denen ein hohes Cybersicherheitsniveau erreicht und aufrechterhalten werden soll.

2) Die NIS-Strategie wird regelmässig, mindestens jedoch alle fünf Jahre, auf der Grundlage wesentlicher Leistungsindikatoren bewertet und falls erforderlich aktualisiert.

3) Die NIS-Strategie ist von der Regierung zu genehmigen. Sie wird nach der Genehmigung auf der Internetseite der Stabsstelle Cyber-Sicherheit veröffentlicht.

IV. Rechtsmittel

Art. 20

Beschwerde

1) Gegen Entscheidungen und Verfügungen der Stabsstelle Cyber-Sicherheit kann binnen 14 Tagen ab Zustellung Beschwerde bei der Beschwerdekommission für Verwaltungsangelegenheiten erhoben werden.

2) Gegen Entscheidungen und Verfügungen der Beschwerdekommission für Verwaltungsangelegenheiten kann binnen 14 Tagen ab Zustellung Beschwerde an den Verwaltungsgerichtshof erhoben werden.

3) Die Überprüfungsbefugnis der Beschwerdekommission für Verwaltungsangelegenheiten sowie des Verwaltungsgerichtshofes beschränkt sich auf Rechts- und Sachfragen. Die Ausübung des Ermessens wird ausschliesslich rechtlich überprüft.

4) Im Übrigen finden auf das Verfahren die Bestimmungen des Gesetzes über die allgemeine Landesverwaltungspflege Anwendung.

V. Strafbestimmungen

Art. 21

Verwaltungsübertretungen

1) Von der Stabstelle Cyber-Sicherheit ist wegen Übertretung mit Busse bis zu 100 000 Franken zu bestrafen, wer als

a) Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen die Pflichten nach Art. 53 Abs. 2 oder 3 der Verordnung (EU) 2019/881 verletzt;

b) Hersteller oder Anbieter von zertifizierten IKT-Produkten, -Diensten oder -Prozessen oder von IKT-Produkten, -Diensten und -Prozessen die Anforderungen nach Art. 55 Abs. 1 oder 2 der Verordnung (EU) 2019/881 nicht einhält;

c) Konformitätsbewertungsstelle gemäss Art. 60 Verordnung (EU) 2019/881 ein europäisches Cybersicherheitszertifikat gemäss Art. 56 Abs. 4 der Verordnung (EU) 2019/881 nicht ordnungsgemäss ausstellt;

d) Inhaber eines europäischen Cybersicherheitszertifikats die Verpflichtungen nach Art. 56 Abs. 8 der Verordnung (EU) 2019/881 verletzt; oder

e) Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, die eine Selbstbewertung der Konformität durchführen, oder als Konformitätsbewertungsstelle gemäss Art. 60 Verordnung (EU) 2019/881 die Überwachung und Beaufsichtigung der Vorschriften der Verordnung (EU) 2019/881 durch die Stabsstelle Cyber-Sicherheit erschwert, behindert oder verunmöglicht.

2) Ordnungswidrig handelt eine wesentliche oder wichtige Einrichtung, wenn sie:

a) nicht die vorgeschriebenen Risikomanagement- und Sicherheitsmassnahmen nach Art. 4 und 5 ergreift;

b) die Berichtspflichten nach Art. 6 verletzt;

c) die nach Art. 14 Abs. 1 Bst. a erforderlichen Informationen, einschliesslich der dokumentierten Sicherheitsmassnahmen, nicht zur Verfügung stellt;

d) Nachweise nach Art. 14 Abs. 1 Bst. b nicht erbringt;

e) Informationen nach Art. 14 Abs. 1 Bst. c gegenüber der Stabsstelle Cyber-Sicherheit nicht offenlegt;

f) Angaben nach Art. 14 Abs. 2 gegenüber der Stabsstelle Cyber-Sicherheit nicht erbringt;

g) die Stabsstelle Cyber-Sicherheit nicht fristgerecht über Aktualisierungen nach Art. 14 Abs. 3 informiert;

g) der Verpflichtung nach Art. 14 Abs. 4 nicht nachkommt;

i) der Verpflichtung spezielle IKT-Produkte, -Dienste und -Prozesse nach Art. 14 Abs. 6 zu verwenden nicht nachkommt;

k) die ordnungsgemässe Durchführung einer Kontrolle nach Art. 17 erschwert, behindert oder verunmöglicht;

l) gegen eine rechtskräftige Verfügung oder Entscheidung der Stabsstelle Cyber-Sicherheit verstösst.

3) Von der Stabsstelle Cyber-Sicherheit werden wesentliche Einrichtungen, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, wegen Verstössen nach Abs. 2 mit Busse bis zu 10 000 000 Franken oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist, bestraft.

4) Von der Stabsstelle Cyber-Sicherheit werden wichtige Einrichtungen, wenn die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, wegen Verstössen nach Abs. 2 mit Busse bis zu 7 000 000 Franken oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, je nachdem, welcher Betrag höher ist, bestraft.

5) Bei der Entscheidung über die Verhängung einer Geldbusse und deren Höhe sind in jedem Einzelfall zumindest folgende Elemente gebührend zu berücksichtigen:

a) die Schwere des Verstosses und die Wichtigkeit der Bestimmungen, gegen die verstossen wurde, wobei Folgendes in allen Fällen als schwerer Verstoss anzusehen ist:

   1. wiederholte Verstösse;

   2. eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen;

   3. eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der Stabsstelle Cyber-Sicherheit gemäss Art. 15 Abs. 5;

   4. die Behinderung von Kontrollen nach Art. 17, die nach der Feststellung eines Verstosses von der Stabsstelle Cyber-Sicherheit oder durch von ihr beauftragte qualifizierte Dritte durchgeführt wurden;

   5. Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagement- und Sicherheitsmassnahmen im Bereich der Cybersicherheit oder Berichtspflichten gemäss den Art. 4 bis 6.

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;

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.

6) Gegen Einrichtungen der öffentlichen Verwaltung werden keine Bussen verhängt.

7) Bei fahrlässiger Begehung werden die Strafobergrenze nach Abs. 1, 3 und 4 auf die Hälfte herabgesetzt.

Art. 22

Verantwortlichkeit

Werden strafbare Handlungen im Geschäftsbetrieb einer juristischen Person, einer Personengesellschaft oder einer Einzelfirma begangen, so finden die Strafbestimmungen auf die Personen Anwendung, die für sie gehandelt haben oder hätten handeln sollen, jedoch unter solidarischer Mithaftung der juristischen Person, der Personengesellschaft oder der Einzelfirma für die Bussen und Kosten.

Art. 23

Besondere Verantwortlichkeit

1) Leitungsorgane wesentlicher und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von Art. 4 und 5 ergriffenen Risikomanagement- und Sicherheitsmassnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

2) Leitungsorgane wesentlicher und wichtiger Einrichtungen sind verpflichtet, selbst an Schulungen teilzunehmen und 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.

3) 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 Vertreter der wesentlichen Einrichtung handelt, ist befugt zu gewährleisten, dass die Einrichtung die Bestimmungen dieses Gesetzes erfüllt.

4) Davon unberührt bleibt die Anwendung des Gesetzes über die Amtshaftung für öffentliche Einrichtungen und für sie handelnde Personen.

VI. Schlussbestimmungen

Art. 24

Durchführungsverordnungen

Die Regierung erlässt die zur Durchführung dieses Gesetzes notwendigen Verordnungen.

Art. 25

Aufhebung bisherigen Rechts

Das Cyber-Sicherheitsgesetz (CSG) vom 4. Mai 2023, LGBl. 2023 Nr. 269, wird aufgehoben.

Art. 26

Inkrafttreten

1) Dieses Gesetz tritt vorbehaltlich Abs. 2 gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Richtlinie (EU) 2022/2555 in das EWR-Abkommen in Kraft.

2) Art. 2 Abs. 1 Bst. c tritt gleichzeitig mit dem Beschluss des Gemeinsamen EWR-Ausschusses betreffend die Übernahme der Verordnung (EU) 2019/881 in das EWR-Abkommen in Kraft.

Anhang 1

(Art. 1)

Sektoren mit hoher Kritikalität

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	• Elektrizitätsunternehmen im Sinne des Art. 2 Ziff. 57 der RL (EU) 2019/944, die die Funktion «Versorgung» im Sinne des Art. 2 Ziff. 12 jener RL wahrnehmen • Verteilernetzbetreiber im Sinne von Art. 2 Ziff. 29 der RL (EU) 2019/944 • Übertragungsnetzbetreiber im Sinne des Art. 2 Ziff. 35 der RL (EU) 2019/944 • Erzeuger im Sinne des Art. 2 Ziff. 38 der RL (EU) 2019/944 • nominierte Strommarktbetreiber im Sinne des Art. 2 Ziff. 8 der Verordnung (EU) 2019/943 • Marktteilnehmer im Sinne des Art. 2 Ziff. 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Art. 2 Ziff. 18, 20 und 59 der RL (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 Art. 2 Ziff. 19 der RL (EU) 2018/2001

		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 Art. 2 Bst. f der RL 2009/119/EG
		d) Erdgas	• Versorgungsunternehmen im Sinne des Art. 2 Ziff. 8 der RL 2009/73/EG • Verteilernetzbetreiber im Sinne des Art. 2 Ziff. 6 der RL 2009/73/EG • Fernleitungsnetzbetreiber im Sinne des Art. 2 Ziff. 4 der RL 2009/73/EG • Betreiber einer Speicheranlage im Sinne des Art. 2 Ziff. 10 der RL 2009/73/EG • Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG • Erdgasunternehmen im Sinne des Art. 2 Ziff. 1 der RL 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 Art. 3 Ziff. 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden • Flughafenleitungsorgane im Sinne des Art. 2 Ziff. 2 der RL 2009/12/EG, Flughäfen im Sinne des Art. 2 Ziff. 1 jener RL, einschliesslich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben • Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Art. 2 Ziff. 1 der Verordnung (EG) Nr. 549/2004 bereitstellen
		b) Schienenverkehr	• Infrastrukturbetreiber im Sinne des Art. 3 Ziff. 2 der RL 2012/34/EU • Eisenbahnunternehmen im Sinne des Art. 3 Ziff. 1 der RL 2012/34/EU, einschliesslich Betreiber einer Serviceeinrichtung im Sinne des Art. 3 Ziff. 12 jener RL
		c) Schifffahrt	• Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 für die Schifffahrt definiert sind, ausschliesslich der einzelnen von diesen Unternehmen betriebenen Schiffe • Leitungsorgane von Häfen im Sinne des Art. 3 Ziff. 1 der RL 2005/65/EG, einschliesslich ihrer Hafenanlagen im Sinne des Art. 2 Ziff. 11 der Verordnung (EG) Nr. 725/2004, sowie

			Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben • Betreiber von Schiffsverkehrsdiensten im Sinne des Art. 3 Bst. o der RL 2002/59/EG
		d) Strassenverkehr	• Strassenverkehrsbehörden im Sinne des Art. 2 Ziff. 12 der Delegierten Verordnung (EU) 2015/962, 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 Art. 4 Ziff. 1 der RL 2010/40/EU
3.	Bankwesen		Kreditinstitute im Sinne von Art. 4 Ziff. 1 der Verordnung (EU) Nr. 575/2013
4.	Finanzmarktinfrastrukturen		• Betreiber von Handelsplätzen im Sinne des Art. 4 Ziff. 24 der RL 2014/65/EU • zentrale Gegenparteien im Sinne des Art. 2 Ziff. 1 der Verordnung (EU) Nr. 648/2012
5.	Gesundheitswesen		• Gesundheitsdienstleister im Sinne des Art. 3 Bst. g der RL 2011/24/EU • EU-Referenzlaboratorien im Sinne des Art. 15 der Verordnung (EU) 2022/2371 • Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Art. 1 Ziff. 2 der RL 2001/83/EG 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 Art. 22 der Verordnung (EU) 2022/123 («Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit») eingestuft werden
6.	Trinkwasser		• Lieferanten von und Unternehmen der Versorgung mit «Wasser für den menschlichen Gebrauch» im Sinne des Art. 2 Ziff. 1 Bst. a der RL (EU) 2020/2184, 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 Art. 2 Ziff. 1, 2 und 3 der RL 91/271/EWG 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 • Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene
11.	Weltraum	Betreiber von Bodeninfrastrukturen, die sich im Eigentum des Fürstentums Liechtenstein oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Anhang 2

(Art. 1)

Sonstige kritische Sektoren

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten im Sinne des Art. 2 Ziff. 1a der RL 97/67/EG, einschliesslich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung im Sinne des Art. 3

			Ziff. 9 der RL 2008/98/EG[11], ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3.	Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne des Art. 3 Ziff. 9 und 14 der Verordnung (EG) Nr. 1907/2006, die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Art. 3 Ziff. 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren
4.	Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen im Sinne des Art. 3 Ziff. 2 der Verordnung (EG) Nr. 178/2002, 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 Art. 2 Ziff. 1 der Verordnung (EU) 2017/745 herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Art. 2 Ziff. 2 der Verordnung (EU) 2017/746 herstellen, mit Ausnahme der unter Anhang I Ziff. 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
		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

[11] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02008L0098-20180705 (EWR: https://www.efta.int/eea-lex/32008L0098)

RICHTLINIEN

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)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([2]),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([4]) war der unionsweite Aufbau von Cybersicherheitskapazitäten, die Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden, und die Sicherstellung der Kontinuität solcher Dienste bei Vorfällen, um so zur Sicherheit der Union und zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft beizutragen.

(2) Seit Inkrafttreten der Richtlinie (EU) 2016/1148 sind erhebliche Fortschritte bei der Stärkung der Cyberresilienz der Union erzielt worden. Die Überprüfung jener Richtlinie hat gezeigt, dass sie als Katalysator für das institutionelle und regulatorische Cybersicherheitskonzept in der Union gedient und ein erhebliches Umdenken bewirkt hat. Durch die Einrichtung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen, die Schaffung nationaler Kapazitäten und die Umsetzung von Regulierungsmaßnahmen für Infrastrukturen und Akteure, die von den einzelnen Mitgliedstaaten als wesentlich eingestuft wurden, wurde mit jener Richtlinie die Vervollständigung der nationalen Rechtsrahmen über die Sicherheit von Netz- und Informationssystemen sichergestellt. Darüber hinaus hat die Richtlinie (EU) 2016/1148 durch die Einrichtung der Kooperationsgruppe und des Netzwerks nationaler Computer-Notfallteams zur Zusammenarbeit auf Unionsebene beigetragen. Ungeachtet dieser Erfolge hat die Überprüfung der Richtlinie (EU) 2016/1148 inhärente Mängel ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern.

(3) Netz- und Informationssysteme sind durch den schnellen digitalen Wandel und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil des Alltags und für den grenzüberschreitenden Austausch geworden. Diese Entwicklung hat zu einer Ausweitung der Cyberbedrohungslage geführt und neue Herausforderungen mit sich gebracht, die in allen Mitgliedstaaten entsprechende koordinierte und innovative Reaktionen erfordern. Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Vorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Vorfälle die Ausübung

([1]) ABl. C 233 vom 16.6.2022, S. 22.
([2]) ABl. C 286 vom 16.7.2021, S. 170.
([3]) Standpunkt des Europäischen Parlaments vom 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.
([4]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanziellen Verlust verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts. Darüber hinaus ist die Cybersicherheit für viele kritische Sektoren eine entscheidende Voraussetzung, um den digitalen Wandel erfolgreich zu bewältigen und die wirtschaftlichen, sozialen und dauerhaften Vorteile der Digitalisierung voll zu nutzen.

(4) Rechtsgrundlage der Richtlinie (EU) 2016/1148 war Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der verstärkte Maßnahmen zur Angleichung der einzelstaatlichen Vorschriften vorsieht, die die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand haben. Die Anforderungen an die Cybersicherheit, die Einrichtungen, die Dienste erbringen oder wirtschaftlich signifikante Tätigkeiten ausüben, auferlegt werden, unterscheiden sich von Mitgliedstaat zu Mitgliedstaat erheblich in Bezug auf die Art der Anforderungen, ihre Detailliertheit und die Art der Aufsicht. Diese Unterschiede verursachen zusätzliche Kosten und führen zu Schwierigkeiten für Einrichtungen, die Waren oder Dienste grenzüberschreitend anbieten. Anforderungen, die von einem Mitgliedstaat auferlegt werden und sich von denen eines anderen Mitgliedstaats unterscheiden oder sogar im Widerspruch zu ihnen stehen, können derartige grenzüberschreitenden Tätigkeiten wesentlich beeinträchtigen. Darüber hinaus dürfte, insbesondere angesichts der Intensität des grenzüberschreitenden Austauschs, eine etwaige unangemessene Gestaltung oder Umsetzung von Cybersicherheitsanforderungen in einem Mitgliedstaat Auswirkungen auf das Cybersicherheitsniveau anderer Mitgliedstaaten haben. Die Überprüfung der Richtlinie (EU) 2016/1148 hat gezeigt, dass die Mitgliedstaaten die Richtlinie sehr unterschiedlich umsetzen, unter anderem in Bezug auf ihren Anwendungsbereich, dessen Abgrenzung weitgehend im Ermessen der Mitgliedstaaten lag. In der Richtlinie (EU) 2016/1148 wurde den Mitgliedstaaten auch ein sehr großer Ermessensspielraum bei der Umsetzung der in der Richtlinie festgelegten Verpflichtungen in Bezug auf die Sicherheit und die Meldung von Sicherheitsvorfällen eingeräumt. Diese Verpflichtungen wurden daher auf nationaler Ebene auf sehr unterschiedliche Weise umgesetzt. Ähnliche Unterschiede gibt es bei der Umsetzung der in der Richtlinie (EU) 2016/1148 enthaltenen Bestimmungen zu Aufsicht und Durchsetzung.

(5) All diese Unterschiede führen zu einer Fragmentierung des Binnenmarkts und können sich nachteilig auf dessen Funktionieren auswirken und aufgrund der Anwendung einer Vielzahl von Maßnahmen insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. Letztendlich könnten diese Unterschiede zu einer höheren Anfälligkeit einiger Mitgliedstaaten gegenüber Cyberbedrohungen führen, deren Auswirkungen auf die gesamte Union übergreifen könnten. Ziel der vorliegenden Richtlinie ist, diese großen Unterschiede zwischen den Mitgliedstaaten zu beseitigen, indem insbesondere Mindestvorschriften für einen funktionierenden und koordinierten Rechtsrahmen festgelegt werden, Mechanismen für die wirksame Zusammenarbeit zwischen den zuständigen Behörden in den einzelnen Mitgliedstaaten vorgesehen werden, die Liste der Sektoren und Tätigkeiten, die Pflichten im Hinblick auf die Cybersicherheit unterliegen, aktualisiert wird und wirksame Abhilfemaßnahmen und Durchsetzungsmaßnahmen, die für die wirksame Durchsetzung dieser Verpflichtungen von entscheidender Bedeutung sind, eingeführt werden. Daher sollte die Richtlinie (EU) 2016/1148 aufgehoben und durch die vorliegende Richtlinie ersetzt werden.

(6) Mit der Aufhebung der Richtlinie (EU) 2016/1148 sollte der Anwendungsbereich nach Sektoren auf einen größeren Teil der Wirtschaft ausgeweitet werden, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind. Diese Richtlinie zielt darauf insbesondere darauf ab, die Mängel bei der Differenzierung zwischen Betreibern wesentlicher Dienste und Anbietern digitaler Dienste zu beheben, die sich als überholt erwiesen hat, da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.

(7) Gemäß der Richtlinie (EU) 2016/1148 waren die Mitgliedstaaten dafür zuständig zu ermitteln, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen. Um die diesbezüglichen großen Unterschiede zwischen den Mitgliedstaaten zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und der Berichtspflichten zu gewährleisten, sollte ein einheitliches Kriterium dafür festgelegt werden, welche Einrichtungen in den Anwendungsbereich der vorliegenden Richtlinie fallen. Dieses Kriterium sollte in der Anwendung des Schwellenwerts für die Größe bestehen, nach der alle Einrichtungen, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG der Kommission ([5]) als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und die in den Sektoren tätig sind und die Art

([5]) Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. Die Mitgliedstaaten sollten auch vorsehen, dass bestimmte Kleinunternehmen und Kleinstunternehmen im Sinne von Artikel 2 Absätze 2 und 3 jenes Anhangs, die bestimmte Kriterien erfüllen, die auf eine Schlüsselrolle für die Gesellschaft, die Wirtschaft oder für bestimmte Sektoren oder Arten von Diensten hindeuten, in den Anwendungsbereich dieser Richtlinie fallen.

(8) Der Ausschluss von Einrichtungen der öffentlichen Verwaltung aus dem Anwendungsbereich dieser Richtlinie sollte für Einrichtungen gelten, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, ausgeübt werden. Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten nur geringfügig mit diesen Bereichen zusammenhängen, sollten jedoch nicht vom Anwendungsbereich dieser Richtlinie ausgenommen werden. Für die Zwecke dieser Richtlinie gelten Einrichtungen mit Regulierungskompetenzen nicht als Einrichtungen, die Tätigkeiten im Bereich der Strafverfolgung ausüben, und sind demnach nicht aus diesem Grunde vom Anwendungsbereich dieser Richtlinie ausgenommen. Einrichtungen der öffentlichen Verwaltung, die gemäß einer internationalen Übereinkunft gemeinsam mit einem Drittland gegründet wurden, sind vom Anwendungsbereich dieser Richtlinie ausgenommen. Diese Richtlinie gilt nicht für diplomatische und konsularische Vertretungen der Mitgliedstaaten in Drittländern oder für deren Netz- und Informationssysteme, sofern sich diese Systeme in den Räumlichkeiten der Mission befinden oder für Nutzer in einem Drittland betrieben werden.

(9) Die Mitgliedstaaten sollten die Möglichkeit haben, die für die Wahrung ihrer wesentlichen Interessen der nationalen Sicherheit und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten zu ermöglichen. Zu diesem Zweck sollten 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, von bestimmten in dieser Richtlinie festgelegten Verpflichtungen in Bezug auf diese Tätigkeiten ausnehmen können. Erbringt eine Einrichtung Dienste ausschließlich für eine Einrichtung der öffentlichen Verwaltung, die vom Anwendungsbereich dieser Richtlinie ausgenommen ist, so sollten die Mitgliedstaaten diese Einrichtung nicht von bestimmten in dieser Richtlinie festgelegten Verpflichtungen in Bezug auf diese Dienste ausnehmen können. Darüber hinaus sollte kein Mitgliedstaat verpflichtet sein, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Interessen der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung widerspräche. Unionsvorschriften und nationale Vorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol sollten in diesem Zusammenhang berücksichtigt werden. Das Traffic Light Protocol ist als eine Mittel zu verstehen, um Informationen über etwaige Einschränkungen im Hinblick auf die weitere Verbreitung von Informationen bereitzustellen. Es wird in fast allen Computer-Notfallteams (computer security incident response teams — CSIRTs) und in einigen Zentren für Informationsanalyse und -weitergabe eingesetzt.

(10) Diese Richtlinie gilt zwar für Einrichtungen, die Tätigkeiten zur Erzeugung von Strom aus Kernkraftwerken ausüben, einige dieser Tätigkeiten können jedoch mit der nationalen Sicherheit in Verbindung stehen. Ist dies der Fall, so sollte ein Mitgliedstaat seine Verantwortung für den Schutz der nationalen Sicherheit in Bezug auf diese Tätigkeiten, einschließlich Tätigkeiten innerhalb der nuklearen Wertschöpfungskette, im Einklang mit den Verträgen wahrnehmen können.

(11) Einige Einrichtungen üben Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, aus und erbringen gleichzeitig Vertrauensdienste. Vertrauensdiensteanbieter, die in den Anwendungsbereich der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([6]) fallen, sollten in den Anwendungsbereich dieser Richtlinie fallen, um das gleiche Niveau der Sicherheitsanforderungen und der Aufsicht zu gewährleisten, wie es zuvor in der genannten Verordnung für Vertrauensdiensteanbieter festgelegt war. Entsprechend dem Ausschluss bestimmter besonderer Dienste von der Verordnung (EU) Nr. 910/2014 findet diese Richtlinie keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden.

([6]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

(12) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates ([7]), einschließlich Anbieter von Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung, Transport oder Zustellung von Postsendungen, einschließlich Abholung durch den Empfänger, anbieten, wobei das Ausmaß ihrer Abhängigkeit von Netz- und Informationssystemen zu berücksichtigen ist. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.

(13) Angesichts der Verschärfung und der zunehmenden Komplexität von Cyberbedrohungen sollten die Mitgliedstaaten bestrebt sein, dafür zu sorgen, dass Einrichtungen, die vom Anwendungsbereich dieser Richtlinie ausgenommen sind, ein hohes Maß an Cybersicherheit erreichen, und die Umsetzung gleichwertiger Maßnahmen für das Risikomanagement im Bereich der Cybersicherheit unterstützen, die dem sensiblen Charakter dieser Einrichtungen Rechnung tragen.

(14) Jede Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie unterliegt dem Unionsrecht zum Datenschutz und zum Schutz der Privatsphäre. Diese Richtlinie lässt insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([8]) und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([9]) unberührt. Diese Richtlinie sollte daher unter anderem nicht die Aufgaben und Befugnisse der Behörden berühren, die für die Überwachung der Einhaltung des geltenden Unionsrechts zum Datenschutz und zum Schutz der Privatsphäre zuständig sind.

(15) Bei Einrichtungen, die für die Zwecke der Einhaltung von Risikomanagementmaßnahmen und der Meldepflichten im Bereich der Cybersicherheit in den Geltungsbereich dieser Richtlinie fallen, sollten zwei Kategorien unterschieden werden: wesentliche Einrichtungen und wichtige Einrichtungen; zu berücksichtigen ist dabei der Grad ihrer Kritikalität in Bezug auf ihren Sektor oder die Art der von ihnen erbrachten Dienste sowie ihre Größe. In diesem Zusammenhang sollten gegebenenfalls einschlägige sektorspezifische Risikobewertungen oder Leitlinien der zuständigen Behörden gebührend berücksichtigt werden. Bei den Aufsichts- und Durchsetzungsregelungen sollte bei diesen beiden Kategorien von Einrichtungen differenziert werden, um ein ausgewogenes Verhältnis zwischen risikobasierten Anforderungen und Pflichten einerseits und dem Verwaltungsaufwand, der sich andererseits aus der Überwachung der Einhaltung ergibt, zu gewährleisten.

(16) Um zu vermeiden, dass Einrichtungen, die Partnerunternehmen haben oder verbundene Unternehmen sind, als wesentliche oder wichtige Einrichtungen betrachtet werden, wenn dies unverhältnismäßig wäre, können die Mitgliedstaaten bei der Anwendung von Artikel 6 Absatz 2 des Anhangs der Empfehlung 2003/361/EG den Grad der Unabhängigkeit einer Einrichtung gegenüber ihren Partnerunternehmen und verbundenen Unternehmen berücksichtigen. Insbesondere können die Mitgliedstaaten berücksichtigen, dass eine Einrichtung in Bezug auf die Netz- und Informationssysteme, die sie bei der Erbringung ihrer Dienste nutzt, und in Bezug auf die von ihr erbrachten Dienste unabhängig von ihren Partnerunternehmen oder verbundenen Unternehmen ist. Auf dieser Grundlage können die Mitgliedstaaten gegebenenfalls davon ausgehen, dass eine solche Einrichtung nicht nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittleres Unternehmen gilt oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels nicht überschreitet, wenn nach Berücksichtigung des Grades der Unabhängigkeit dieser Einrichtung davon ausgegangen worden wäre, dass sie nicht als mittleres Unternehmen gilt oder diese Schwellenwerte nicht überschreitet, falls nur ihre eigenen Daten berücksichtigt worden wären. Die in dieser Richtlinie festgelegten Verpflichtungen von Partnerunternehmen und verbundenen Unternehmen, die in den Anwendungsbereich dieser Richtlinie fallen, bleiben davon unberührt.

(17) Die Mitgliedstaaten sollten beschließen können, dass Einrichtungen, die vor Inkrafttreten dieser Richtlinie gemäß der Richtlinie (EU) 2016/1148 als Betreiber wesentlicher Dienste ermittelt wurden, als wesentliche Einrichtungen gelten.

([7]) Richtlinie 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstequalität (ABl. L 15 vom 21.1.1998, S. 14).

([8]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([9]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

(18) Um für einen klaren Überblick über die in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen zu sorgen, sollten die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, erstellen. Zu diesem Zweck sollten die Mitgliedstaaten die Einrichtungen dazu verpflichten, den zuständigen Behörden mindestens die folgenden Informationen zu übermitteln, nämlich Name, Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adressen, IP-Adressbereiche und Telefonnummern der Einrichtung, und gegebenenfalls betreffender Sektor und Teilsektor gemäß den Anhängen, sowie gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie in den Anwendungsbereich dieser Richtlinie fallende Dienste erbringen. Zu diesem Zweck sollte die Kommission mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) unverzüglich Leitlinien und Vorlagen für die Verpflichtungen zur Übermittlung von Informationen bereitstellen. Um die Erstellung und Aktualisierung der Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, zu erleichtern, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Mechanismen für die Registrierung von Einrichtungen einzurichten. Bestehen Register auf nationaler Ebene, können die Mitgliedstaaten geeignete Mechanismen beschließen, die die Identifizierung von Einrichtungen ermöglichen, die in den Anwendungsbereich dieser Richtlinie fallen.

(19) Die Mitgliedstaaten sollten dafür verantwortlich sein, der Kommission mindestens die Zahl der wesentlichen und wichtigen Einrichtungen für jeden in den Anhängen genannten Sektor und Teilsektor sowie relevante Informationen über die Zahl der ermittelten Einrichtungen und die Bestimmungen dieser Richtlinie, auf deren Grundlage sie ermittelt wurden, und die Art der von ihnen erbrachten Dienste zu übermitteln. Die Mitgliedstaaten werden aufgefordert, mit der Kommission Informationen über wesentliche und wichtige Einrichtungen und – im Falle eines Cybersicherheitsvorfalls großen Ausmaßes – relevante Informationen wie den Namen der betreffenden Einrichtung auszutauschen.

(20) Die Kommission sollte in Zusammenarbeit mit der Kooperationsgruppe und nach Konsultation der einschlägigen Interessenträger Leitlinien für die Anwendung der für Kleinstunternehmen und kleine Unternehmen geltenden Kriterien bereitstellen, um zu bewerten, ob sie in den Anwendungsbereich dieser Richtlinie fallen. Die Kommission sollte auch dafür sorgen, dass Kleinstunternehmen und Kleinunternehmen, die in den Anwendungsbereich dieser Richtlinie fallen, eine angemessene Anleitung erhalten. Die Kommission sollte mit Unterstützung der Mitgliedstaaten den Kleinstunternehmen und Kleinunternehmen diesbezügliche Informationen zur Verfügung stellen.

(21) Die Kommission könnte Leitlinien herausgeben, um die Mitgliedstaaten bei der Umsetzung der Bestimmungen dieser Richtlinie über den Anwendungsbereich und bei der Bewertung der Verhältnismäßigkeit der im Rahmen dieser Richtlinie zu treffenden Maßnahmen zu unterstützen, insbesondere in Bezug auf Einrichtungen mit komplexen Geschäftsmodellen oder Betriebsumgebungen, wobei eine Einrichtung gleichzeitig die Kriterien für wesentliche und für wichtige Einrichtungen erfüllen kann oder gleichzeitig Tätigkeiten, die in den Anwendungsbereich dieser Richtlinie fallen, und andere Tätigkeiten, die nicht in den Anwendungsbereich dieser Richtlinie fallen, ausführen kann.

(22) In dieser Richtlinie wird das Grundniveau für Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit für die in den Anwendungsbereich der Richtlinie fallenden Sektoren festgelegt. Wenn zusätzliche sektorspezifische Rechtsakte der Union über Maßnahmen zum Cybersicherheitsrisikomanagement und Berichtspflichten für notwendig erachtet werden, um in der gesamten Union ein hohes Maß an Cybersicherheit zu gewährleisten, sollte die Kommission — zur Vermeidung einer Fragmentierung der Cybersicherheitsbestimmungen von Rechtsakten der Union — prüfen, ob diese weiteren Bestimmungen im Rahmen eines Durchführungsrechtsakts gemäß dieser Richtlinie festgelegt werden könnten. Sollte sich ein solcher Durchführungsrechtsakt zu diesem Zweck nicht eignen, so könnten sektorspezifische Rechtsakte der Union dazu beitragen, dass in der gesamten Union ein hohes Maß an Cybersicherheit gewährleistet ist und gleichzeitig den Besonderheiten und Komplexitäten der betreffenden Sektoren in vollem Umfang Rechnung getragen wird. Daher schließt die vorliegende Richtlinie nicht aus, dass zusätzliche sektorspezifische Rechtsakte der Union zu Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit, die der Notwendigkeit eines umfassenden und kohärenten Cybersicherheitsrahmens gebührend Rechnung tragen, erlassen werden. Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

(23) Wenn wesentliche oder wichtige Einrichtungen gemäß den Bestimmungen eines sektorspezifischen Rechtsakts der Union entweder Risikomanagementmaßnahmen im Bereich der Cybersicherheit ergreifen oder erhebliche Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen zumindest gleichwertig sind, sollten diese Bestimmungen, einschließlich der

Bestimmungen über Aufsicht und Durchsetzung, keine Anwendung auf solche Einrichtungen finden. Wenn ein sektorspezifischer Rechtsakt der Union nicht für alle in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen eines bestimmten Sektors gilt, sollten die einschlägigen Bestimmungen dieser Richtlinie weiterhin im Falle der Einrichtungen zur Anwendung kommen, die nicht unter diesen Rechtsakt fallen.

(24) Wenn wesentliche oder wichtige Einrichtungen nach den Bestimmungen eines sektorspezifischen Rechtsakts der Union verpflichtet sind, Berichtspflichten zu erfüllen, die mindestens die gleiche Wirkung wie die in dieser Richtlinie festgelegten Berichtspflichten haben, sollte dafür gesorgt werden, dass Meldungen von Sicherheitsvorfällen kohärent und wirksam bearbeitet werden. Zu diesem Zweck sollten die Bestimmungen über die Meldung von Sicherheitsvorfällen des sektorspezifischen Rechtsakts der Union den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen für Cybersicherheit (zentrale Anlaufstelle) gemäß dieser Richtlinie einen sofortigen Zugang zu den gemäß dem sektorspezifischen Rechtsakt der Union übermittelten Meldungen von Sicherheitsvorfällen ermöglichen. Ein solcher sofortiger Zugang kann insbesondere gewährt werden, wenn Meldungen von Sicherheitsvorfällen unverzüglich an das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle gemäß dieser Richtlinie weitergeleitet werden. Gegebenenfalls sollten die Mitgliedstaaten einen automatischen und direkten Meldemechanismus einrichten, der einen systematischen und sofortigen Informationsaustausch mit den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen für die Bearbeitung solcher Meldungen von Sicherheitsvorfällen sicherstellt. Um die Berichterstattung zu vereinfachen und den Mechanismus der automatischen und direkten Berichterstattung umzusetzen, könnten die Mitgliedstaaten im Einklang mit dem sektorspezifischen Rechtsakt der Union eine zentrale Anlaufstelle nutzen.

(25) In sektorspezifischen Rechtsakten der Union, in denen Risikomanagementmaßnahmen oder Berichtspflichten im Bereich der Cybersicherheit vorgesehen sind, die in ihrer Wirkung den in dieser Richtlinie festgelegten entsprechenden Maßnahmen und Pflichten mindestens gleichwertig sind, könnte vorgesehen werden, dass die gemäß dieser Rechtsakte zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf solche Maßnahmen oder Pflichten mit Unterstützung der zuständigen Behörden gemäß der vorliegenden Richtlinie ausüben. Die betreffenden zuständigen Behörden könnten zu diesem Zweck Kooperationsvereinbarungen schließen. In solchen Kooperationsvereinbarungen könnten unter anderem die Verfahren für die Koordinierung der Aufsichtstätigkeiten festgelegt werden, einschließlich der Verfahren für im Einklang mit nationalem Recht durchzuführende Untersuchungen und Prüfungen vor Ort und eines Mechanismus für den Austausch einschlägiger Informationen zwischen den zuständigen Behörden über Aufsicht und Durchsetzung, wozu auch der Zugang zu Cyberinformationen gehört, der von den zuständigen Behörden gemäß dieser Richtlinie beantragt wird.

(26) Wenn sektorspezifische Rechtsakte der Union Einrichtungen zur Meldung erheblicher Cyberbedrohungen verpflichten oder ihnen entsprechende Anreize bieten, sollten die Mitgliedstaaten auch fördern, dass erhebliche Cyberbedrohungen den CSIRTs, den zuständigen Behörden oder den zentralen Anlaufstellen gemäß dieser Richtlinie gemeldet werden, um dafür zu sorgen, dass diesen Stellen die Cyberbedrohungslage besser bewusst ist, und sie in die Lage zu versetzen, wirksam und rechtzeitig zu reagieren, falls die erheblichen Cyberbedrohungen eintreten sollten.

(27) In künftigen sektorspezifischen Rechtsakten der Union sollte den in dieser Richtlinie festgelegten Begriffsbestimmungen und dem Aufsichts- und Durchsetzungsrahmen gebührend Rechnung getragen werden.

(28) Die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([10]) sollte im Zusammenhang mit der vorliegenden Richtlinie als sektorspezifischer Rechtsakt der Union in Bezug auf Finanzunternehmen betrachtet werden. Anstelle der Bestimmungen in der vorliegenden Richtlinie sollten die Bestimmungen der Verordnung (EU) 2022/2554 gelten, die sich auf Risikomanagement im Bereich der Informations- und Kommunikationstechnologien (IKT), das Management von IKT-bezogenen Vorfällen und insbesondere die Meldung von schwerwiegenden IKT-bezogenen Vorfällen sowie die Prüfung der digitalen Betriebsstabilität, Vereinbarungen über den Informationsaustausch und Risiken durch IKT-Drittanbieter beziehen. Die Mitgliedstaaten sollten daher die Bestimmungen der vorliegenden Richtlinie, die sich auf Cybersicherheitsrisikomanagement und Berichtspflichten sowie Aufsicht und Durchsetzung beziehen, nicht auf Finanzunternehmen anwenden, die unter jene Verordnung fallen. Gleichzeitig ist es wichtig, im Rahmen der vorliegenden Richtlinie eine enge Beziehung zum und den Informationsaustausch mit dem Finanzsektor aufrechtzuerhalten. Zu diesem Zweck ist es gemäß der Verordnung (EU) 2022/2554 zulässig, dass die Europäischen Aufsichtsbehörden und die gemäß der Verordnung (EU) 2022/2554 zuständigen nationalen Behörden sich an der Tätigkeit der Kooperationsgruppe beteiligen und mit den zentralen Anlaufstellen sowie den

([10]) Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Betriebsstabilität digitaler Systeme im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (siehe Seite 1 dieses Amtsblatts).

nationalen CSIRTs und den zuständigen Behörden gemäß dieser Richtlinie Informationen austauschen und zusammenarbeiten Die gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden sollten auch Einzelheiten über schwerwiegende IKT-bezogenen Vorfällen und, gegebenenfalls, erhebliche Cyberbedrohungen auch an die CSIRTs, die zuständigen Behörden oder an die gemäß der vorliegenden Richtlinie benannten zentralen Anlaufstellen übermitteln. Dies lässt sich erreichen, indem ein unmittelbarer Zugang zu Meldungen von Vorfällen und ihre direkte Weiterleitung oder über eine zentrale Anlaufstelle für die Meldung von Vorfällen ermöglicht wird. Darüber hinaus sollten die Mitgliedstaaten den Finanzsektor weiterhin in ihre Cybersicherheitsstrategien einbeziehen, und die CSIRTs können den Finanzsektor bei ihren Tätigkeiten einbeziehen.

(29) Um Lücken und Überschneidungen bei Luftverkehrseinrichtungen auferlegten Cybersicherheitsverpflichtungen zu vermeiden, sollten die gemäß den Verordnungen (EG) Nr. 300/2008 ([11]) und (EU) 2018/1139 ([12]) des Europäischen Parlaments und des Rates benannten nationalen Behörden und die gemäß dieser Richtlinie zuständigen Behörden bei der Umsetzung von Maßnahmen zum Cybersicherheitsrisikomanagement und der Aufsicht über die Einhaltung dieser Maßnahmen auf nationaler Ebene zusammenarbeiten. Die Einhaltung der Sicherheitsanforderungen durch eine Einrichtung, die in den Verordnungen (EG) Nr. 300/2008 und (EU) 2018/1139 sowie in den gemäß diesen Verordnungen erlassenen einschlägigen delegierten Rechtsakten und Durchführungsrechtsakten festgelegt sind, könnte von den gemäß dieser Richtlinie zuständigen Behörden als Einhaltung der entsprechenden Anforderungen dieser Richtlinie erachtet werden.

(30) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates ([13]) und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Darüber hinaus sollte jeder Mitgliedstaat sicherstellen, dass seine nationale Cybersicherheitsstrategie einen politischen Rahmen für eine verstärkte Koordinierung innerhalb dieses Mitgliedstaaten zwischen seinen gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 beim Informationsaustausch über Risiken, Cyberbedrohungen und Sicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle sowie bei der Wahrnehmung von Aufsichtsaufgaben vorsieht. Die gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 sollten zusammenarbeiten und unverzüglich Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken und Sicherheitsvorfälle sowie nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle, die kritische Einrichtungen beeinträchtigen, einschließlich der von kritischen Einrichtungen ergriffenen Cybersicherheitsmaßnahmen und physischen Maßnahmen sowie der Ergebnisse der bezüglich dieser Einrichtungen durchgeführten Aufsichtstätigkeiten.

Um die Aufsichtstätigkeiten zwischen den nach der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 zu straffen und den Verwaltungsaufwand für die betreffenden Einrichtungen so gering wie möglich zu halten, sollten diese zuständigen Behörden zudem bestrebt sein, die Vorlagen für die Meldung von Sicherheitsvorfällen und die Aufsichtsverfahren zu harmonisieren. Gegebenenfalls sollten die gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden die gemäß der vorliegenden Richtlinie zuständigen Behörden ersuchen können, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine Einrichtung, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtung eingestuft wird, auszuüben. Die gemäß der vorliegenden Richtlinie zuständigen Behörden und denen gemäß Richtlinie (EU) 2022/2557 sollten zu diesem Zweck nach Möglichkeit in Echtzeit zusammenarbeiten und Informationen austauschen.

(31) Einrichtungen im Bereich digitale Infrastruktur beruhen im Wesentlichen auf Netz- und Informationssystemen; aus diesem Grund sollte in den Verpflichtungen, die diesen Einrichtungen gemäß dieser Richtlinie im Rahmen ihrer Risikomanagementmaßnahmen und Berichtspflichten im Bereich Cybersicherheit auferlegt werden, umfassend auf die physische Sicherheit dieser Systeme eingegangen werden. Da diese Angelegenheiten Gegenstand der vorliegenden Richtlinie sind, gelten die in den Kapiteln III, IV und VI der Richtlinie (EU) 2022/2557 festgelegten Verpflichtungen nicht für solche Einrichtungen.

([11]) Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72).

([12]) Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates (ABl. L 212 vom 22.8.2018, S. 1).

([13]) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (siehe Seite164 dieses Amtsblatts).

(32) Die Aufrechterhaltung und Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (domain name system — DNS) ist ein Schlüsselfaktor für die Wahrung der Integrität des Internets und von entscheidender Bedeutung für dessen kontinuierlichen und stabilen Betrieb, von dem die digitale Wirtschaft und Gesellschaft abhängig ist. Daher sollte die vorliegende Richtlinie für Namenregister der Domäne oberster Stufe (top-level-domain — TLD) und DNS-Diensteanbieter gelten, die als Einrichtungen zu verstehen sind, die öffentlich zugängliche rekursive Dienste zur Auflösung von Domänennamen für Internet-Endnutzer oder autoritative Dienste zur Auflösung von Domänennamen erbringen. Diese Richtlinie sollte nicht für Root-Namenserver gelten.

(33) Cloud-Computing-Dienste sollten digitale Dienste umfassen, die auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind. Zu Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Betriebssysteme, Software, Speicher, Anwendungen und Dienste. Zu den Dienstmodellen des Cloud-Computing gehören unter anderem IaaS (Infrastructure as a Service, PaaS (Platform as a Service), SaaS (Software as a Service) und NaaS (Network as a Service). Die Bereitstellungsmodelle für Cloud-Computing sollten die private, die gemeinschaftliche, die öffentliche und die hybride Cloud umfassen. Die Cloud-Computing-Dienst- und Bereitstellungsmodelle haben dieselbe Bedeutung wie die in der Norm ISO/IEC 17788:2014 definierten Dienst- und Bereitstellungsmodelle. Dass sich der Cloud-Computing-Nutzer selbst ohne Interaktion mit dem Anbieter von Cloud-Computing-Diensten Rechenkapazitäten wie Serverzeit oder Netzwerkspeicherplatz zuweisen kann, könnte als Verwaltung auf Abruf beschrieben werden.

Der Begriff „umfassender Fernzugang“ wird verwendet, um zu beschreiben, dass die Cloud-Kapazitäten über das Netz bereitgestellt und über Mechanismen zugänglich gemacht werden, die den Einsatz heterogener Thin- oder Thick-Client-Plattformen (einschließlich Mobiltelefonen, Tablets, Laptops und Arbeitsplatzrechnern) fördern. Der Begriff „skalierbar“ bezeichnet Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Dienstes flexibel zugeteilt werden, damit Nachfrageschwankungen bewältigt werden können. Der Begriff „elastischer Pool“ wird verwendet, um Rechenressourcen zu beschreiben, die entsprechend der Nachfrage bereitgestellt und freigegeben werden, damit die Menge der verfügbaren Ressourcen je nach Arbeitsaufkommen rasch erhöht oder reduziert werden kann. Der Begriff „gemeinsam nutzbar“ wird verwendet, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, die über einen gemeinsamen Zugang auf den Dienst zugreifen, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst über dieselbe elektronische Ausrüstung erbracht wird. Der Begriff „verteilt“ wird verwendet, um Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.

(34) Angesichts des Aufkommens innovativer Technologien und neuer Geschäftsmodelle dürften auf dem Binnenmarkt neue Dienst- und Bereitstellungsmodelle für Cloud-Computing entstehen, um den sich wandelnden Kundenbedürfnissen gerecht zu werden. In diesem Zusammenhang können Cloud-Computing-Dienste in hochgradig verteilter Form, noch näher am Ort der Datengenerierung oder -sammlung, erbracht werden, wodurch vom traditionellen Modell zu einem hochgradig verteilten Modell („Edge-Computing“) übergegangen wird.

(35) Dienste, die von Anbietern von Rechenzentrumsdiensten angeboten werden, werden möglicherweise nicht immer in Form eines Cloud-Computing-Diensts erbracht. Dementsprechend sind Rechenzentren möglicherweise nicht immer Teil einer Cloud-Computing-Infrastruktur. Um allen Risiken für die Sicherheit von Netz- und Informationssystemen zu begegnen, sollte die vorliegende Richtlinie daher für Anbieter von Rechenzentrumsdiensten gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienste umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie (IT) und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden. Der Begriff „Rechenzentrumsdienst“ sollte nicht für interne Rechenzentren, die sich im Besitz der betreffenden Einrichtung befinden und von der betreffenden Einrichtung für eigene Zwecke betrieben werden.

(36) Forschungstätigkeiten spielen eine Schlüsselrolle bei der Entwicklung neuer Produkte und Prozesse. Viele dieser Tätigkeiten werden von Einrichtungen durchgeführt, die ihre Forschungsergebnisse zu kommerziellen Zwecken teilen, verbreiten oder nutzen. Diese Einrichtungen können daher wichtige Akteure in Wertschöpfungsketten sein, was die Sicherheit ihrer Netz- und Informationssysteme zu einem integralen Bestandteil der allgemeinen

Cybersicherheit des Binnenmarkts macht. Unter Forschungseinrichtungen sind unter anderem Einrichtungen zu verstehen, die sich im Wesentlichen auf die Durchführung von angewandter Forschung oder experimenteller Entwicklung im Sinne des Frascati-Handbuchs der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung von 2015 (Leitlinien zur Erfassung von Daten zu Forschung und experimenteller Entwicklung sowie zur entsprechenden Berichterstattung) konzentrieren, um ihre Ergebnisse für kommerzielle Zwecke wie die Herstellung oder Entwicklung eines Produkts oder eines Verfahrens, die Erbringung eines Dienstes, oder dessen Vermarktung zu nutzen.

(37) Die wachsenden gegenseitigen Abhängigkeiten sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend interdependenten Dienstleistungsnetzes, das zentrale Infrastrukturen in der gesamten Union nutzt, und zwar in Sektoren wie z.B. Energie, Verkehr, digitale Infrastruktur, Trinkwasser und Abwasser, Gesundheit, bestimmten Bereichen der öffentlichen Verwaltung sowie im Weltraumsektor, soweit es um die Erbringung bestimmter Dienste geht, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; damit sind Infrastrukturen ausgenommen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihres Weltraumprogramms verwaltet oder betrieben werden. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können. Die verstärkten Cyberangriffe während der COVID-19-Pandemie haben gezeigt, wie anfällig zunehmend interdependente Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

(38) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, eine oder mehr als eine nationale Behörde zu benennen oder einzurichten, die für die Cybersicherheit und die Aufsichtsaufgaben gemäß der vorliegenden Richtlinie zuständig sind.

(39) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation zwischen Behörden und um die wirksame Umsetzung der vorliegenden Richtlinie zu ermöglichen, ist es notwendig, dass jeder Mitgliedstaat eine zentrale Anlaufstelle benennt, die für die Koordinierung im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist.

(40) Die zentralen Anlaufstellen sollten für eine wirksame grenzüberschreitende Zusammenarbeit mit den zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Kommission und der ENISA sorgen. Die zentralen Anlaufstellen sollten daher beauftragt werden, Meldungen über erhebliche Sicherheitsvorfälle mit grenzüberschreitenden Auswirkungen auf Ersuchen des CSIRT oder der zuständigen Behörde an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten. Auf nationaler Ebene sollten die zentralen Anlaufstellen eine reibungslose sektorübergreifende Zusammenarbeit mit anderen zuständigen Behörden ermöglichen. Die zentralen Anlaufstellen könnten auch relevante Informationen über Vorfälle, die Finanzeinrichtungen betreffen, von den gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden entgegennehmen, die sie gegebenenfalls gemäß der vorliegenden Richtlinie an die CSIRTs oder die zuständigen Behörden weiterleiten können sollten.

(41) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten verfügen, um Sicherheitsvorfälle und Risiken zu verhüten und zu erkennen, darauf zu reagieren und um ihre Auswirkungen abzuschwächen. Die Mitgliedstaaten sollten daher ein oder mehrere CSIRTs gemäß dieser Richtlinie benennen und sicherstellen, dass sie über angemessene Ressourcen und technische Kapazitäten verfügen. Die CSIRTs sollten die Anforderungen im Sinne dieser Richtlinie erfüllen, damit wirksame und kompatible Kapazitäten zur Bewältigung von Sicherheitsvorfällen und Risiken und eine effiziente Zusammenarbeit auf Unionsebene gewährleistet sind. Die Mitgliedstaaten sollten auch bestehende Computer-Notfallteams (CERTs) als CSIRTs benennen können. Um das Vertrauensverhältnis zwischen den Einrichtungen und den CSIRTs zu stärken, sollten die Mitgliedstaaten in Fällen, in denen ein CSIRT Teil einer zuständigen Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs, insbesondere in Bezug auf den Informationsaustausch und die den Einrichtungen gewährten Unterstützung, und den Aufsichtstätigkeiten der zuständigen Behörden in Erwägung ziehen können.

(42) Die CSIRTs sind mit der Bewältigung von Sicherheitsvorfällen betraut. Das umfasst die Verarbeitung großer Mengen in einigen Fällen sensibler Daten. Die Mitgliedstaaten sollten dafür sorgen, dass die CSIRTs über eine Infrastruktur für den Informationsaustausch und die Verarbeitung von Informationen sowie über gut ausgestattetes Personal verfügen, womit die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeiten gewährleistet wird. Die CSIRTs könnten in diesem Zusammenhang auch Verhaltenskodizes annehmen.

(43) In Bezug auf personenbezogene Daten sollten die CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 im Namen und auf Ersuchen einer wesentlichen oder wichtigen Einrichtung eine proaktive Überprüfung der für die Bereitstellung der Dienste der Einrichtungen verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten gegebenenfalls für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten sollten die ENISA um Unterstützung bei der Einsetzung ihrer CSIRTs ersuchen können.

(44) Die CSIRTs sollten in der Lage sein, auf Ersuchen einer wesentlichen oder wichtigen Einrichtung die mit dem Internet verbundenen Anlagen innerhalb und außerhalb der Geschäftsräume zu überwachen, um das organisatorische Gesamtrisiko der Einrichtung für neu ermittelte Sicherheitslücken in der Lieferkette oder kritische Schwachstellen zu ermitteln, zu verstehen und zu verwalten. Die Einrichtung sollte dazu angehalten werden, dem CSIRT mitzuteilen, ob es eine privilegierte Verwaltungsschnittstelle betreibt, da dies die Geschwindigkeit der Durchführung von Abhilfemaßnahmen beeinträchtigen könnte.

(45) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRTs-Netzwerk an internationalen Kooperationsnetzen beteiligen können. Zur Erfüllung ihrer Aufgaben sollten die CSIRTs und die zuständigen Behörden daher in der Lage sein, Informationen, einschließlich personenbezogener Daten, mit nationalen Computer-Notfallteams oder zuständigen Behörden von Drittländern auszutauschen, sofern die Bedingungen des Datenschutzrechts der Union für die Übermittlung personenbezogener Daten an Drittländer, unter anderem gemäß Artikel 49 der Verordnung (EU) 2016/679, erfüllt sind.

(46) Es ist von wesentlicher Bedeutung, dass angemessene Ressourcen bereitgestellt werden, um die Ziele dieser Richtlinie zu erreichen und es den zuständigen Behörden und den CSIRTs zu ermöglichen, die dort festgelegten Aufgaben zu erfüllen. Die Mitgliedstaaten können auf nationaler Ebene einen Finanzierungsmechanismus zur Deckung der Ausgaben einführen, die im Zusammenhang mit der Wahrnehmung der Aufgaben der in dem Mitgliedstaat gemäß dieser Richtlinie für Cybersicherheit zuständigen öffentlichen Einrichtungen erforderlich sind. Ein solcher Mechanismus sollte im Einklang mit dem Unionsrecht stehen, verhältnismäßig und diskriminierungsfrei sein und den unterschiedlichen Ansätzen für die Bereitstellung sicherer Dienste Rechnung tragen.

(47) Das CSIRTs-Netzwerk sollte weiterhin zur Stärkung des Vertrauens beitragen und eine rasche und wirksame operative Zusammenarbeit zwischen den Mitgliedstaaten fördern. Um die operative Zusammenarbeit auf Unionsebene zu verbessern, sollte das CSIRTs-Netzwerk in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa Europol, zur Teilnahme an seiner Arbeit einzuladen.

(48) Um ein hohes Cybersicherheitsniveau zu erreichen und aufrechtzuerhalten, sollten die gemäß dieser Richtlinie erforderlichen nationalen Cybersicherheitsstrategien aus kohärenten Rahmen bestehen, in denen strategische Ziele und Prioritäten im Bereich der Cybersicherheit und die zu ihrer Verwirklichung erforderliche Governance festgelegt werden. Diese Strategien können aus einem oder mehreren legislativen oder nichtlegislativen Instrumenten bestehen.

(49) Maßnahmen für die Cyberhygiene bilden die Grundlage für den Schutz von Netz- und Informationssysteminfrastrukturen, Hardware, Software und Online-Anwendungssicherheit sowie von Geschäfts- oder Endnutzerdaten, derer sich Einrichtungen bedienen. Maßnahmen für die Cyberhygiene, die eine Reihe von grundlegenden Verfahren umfassen, wie z. B. Software- und Hardware-Updates, Passwortänderungen, die Verwaltung neuer Installationen, die Einschränkung von Zugriffskonten auf Administratorenebene und die Sicherung von Daten, ermöglichen einen proaktiven Rahmen für die Bereitschaft und die allgemeine Sicherheit im Falle von Sicherheitsvorfällen oder Cyberbedrohungen. Die ENISA sollte die Cyberhygienemaßnahmen der Mitgliedstaaten überwachen und analysieren.

(50) Sensibilisierung für Cybersicherheit und Cyberhygiene sind von entscheidender Bedeutung, um das Cybersicherheitsniveau in der Union zu erhöhen, insbesondere angesichts der wachsenden Zahl vernetzter Geräte, die zunehmend bei Cyberangriffen eingesetzt werden. Es sollten Anstrengungen unternommen werden, um das allgemeine Bewusstsein für die Risiken im Zusammenhang mit derartigen Produkten zu schärfen, wobei Bewertungen auf Unionsebene dazu beitragen könnten, für ein gemeinsames Verständnis dieser Risiken im Binnenmarkt zu sorgen.

(51) Die Mitgliedstaaten sollten den Einsatz innovativer Technologien, einschließlich künstlicher Intelligenz, fördern, deren Einsatz die Aufdeckung und Verhütung von Cyberangriffen verbessern könnte, sodass Ressourcen wirksamer gegen Cyberangriffe genutzt werden können. Die Mitgliedstaaten sollten daher im Rahmen ihrer nationalen Cybersicherheitsstrategie Tätigkeiten im Bereich Forschung und Entwicklung fördern, um die Nutzung derartiger Technologien, insbesondere solcher, die sich auf automatisierte oder halbautomatisierte Instrumente für die Cybersicherheit beziehen, und gegebenenfalls den Austausch von Daten zu erleichtern, die für die Schulung und Verbesserung dieser Technologien erforderlich sind. Der Einsatz innovativer Technologien, einschließlich künstlicher Intelligenz, sollte in Einklang mit dem Datenschutzrecht der Union stehen, einschließlich der Datenschutzgrundsätze der Datengenauigkeit, Datenminimierung, Fairness und Transparenz sowie Datensicherheit, wie z. B. modernste Verschlüsselung. Die in der Verordnung (EU) 2016/679 festgelegten Anforderungen des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen sollten voll ausgeschöpft werden.

(52) Open-Source-Cybersicherheitswerkzeuge und -Anwendungen können zu einem höheren Maß an Offenheit beitragen und sich positiv auf die Effizienz industrieller Innovationen auswirken. Offene Standards erleichtern die Interoperabilität zwischen Sicherheitstools, was der Sicherheit der Interessenträger aus der Industrie zugutekommt. Open-Source-Cybersicherheitswerkzeuge und -anwendungen können die breitere Entwicklergemeinschaft nutzen und damit eine Diversifizierung der Anbieter ermöglichen. Open-Source kann zu einem transparenteren Verfahren für die Überprüfung von Werkzeugen für die Cybersicherheit und zu einem von der Gemeinschaft gesteuerten Prozess der Aufdeckung von Schwachstellen führen. Die Mitgliedstaaten sollten daher den Einsatz von Open-Source-Software und offenen Standards fördern können, indem sie Maßnahmen zur Nutzung offener Daten und Open-Source als Teil der Sicherheit durch Transparenz verfolgen. Maßnahmen zur Förderung der Einführung und nachhaltigen Nutzung von Open-Source-Cybersicherheitswerkzeugen sind besonders für kleine und mittlere Unternehmen wichtig, bei denen erhebliche Implementierungskosten anfallen, die durch die Reduzierung des Bedarfs an spezifischen Anwendungen oder Werkzeugen minimiert werden könnten.

(53) Versorgungsunternehmen sind zunehmend an digitale Netze in Städten angeschlossen, um die städtischen Verkehrsnetze zu verbessern, die Wasserversorgungs- und Abfallentsorgungseinrichtungen zu verbessern und die Effizienz der Beleuchtung und der Beheizung von Gebäuden zu erhöhen. Diese digitalisierten Versorgungsunternehmen sind anfällig für Cyberangriffe und es besteht aufgrund ihrer Vernetzung die Gefahr, dass den Bürgern im Falle eines erfolgreichen Cyberangriffs schwerwiegend geschadet wird. Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Cybersicherheitsstrategie eine Strategie entwickeln, die sich mit der Entwicklung solcher vernetzten oder intelligenten Städte und deren potenziellen Auswirkungen auf die Gesellschaft befasst.

(54) In den letzten Jahren war die Union mit einem exponentiellen Anstieg von Ransomware-Angriffen konfrontiert, bei denen Daten und Systeme durch Malware verschlüsselt werden und eine Lösegeldzahlung für die Freigabe verlangt wird. Die zunehmende Häufigkeit und Schwere von Ransomware-Angriffen kann auf verschiedene Faktoren zurückgeführt werden, wie z. B. unterschiedliche Angriffsmuster, kriminelle Geschäftsmodelle im Zusammenhang mit „Ransomware als Dienst“ und Kryptowährungen, die Forderung nach Lösegeld und die Zunahme von Angriffen auf die Lieferkette. Die Mitgliedstaaten sollten eine Strategie zum Vorgehen gegen die zunehmende Häufigkeit von Ransomware-Angriffen als Teil ihrer nationalen Cybersicherheitsstrategie ergreifen.

(55) Öffentlich-private Partnerschaften (ÖPP) im Bereich der Cybersicherheit können einen angemessenen Rahmen für den Wissensaustausch, die Weitergabe von bewährten Verfahren und die Schaffung einer gemeinsamen Verständnisebene zwischen den Beteiligten bieten. Die Mitgliedstaaten sollten Maßnahmen fördern, die die Einrichtung von cybersicherheitsspezifischen ÖPP unterstützen. Diese Maßnahmen sollten unter anderem den Anwendungsbereich und die beteiligten Akteure, das Verwaltungsmodell, die verfügbaren Finanzierungsoptionen und das Zusammenspiel der beteiligten Akteure in Bezug auf ÖPP präzisieren. ÖPP können das Fachwissen privatwirtschaftlicher Einrichtungen nutzen, um die zuständigen Behörden bei der Entwicklung modernster Dienste und Prozesse zu unterstützen, unter anderem in den Bereichen Informationsaustausch, Frühwarnungen, Übungen zu Cyberbedrohungen und -vorfällen, Krisenmanagement und Resilienzplanung.

(56) Die Mitgliedstaaten sollten in ihren nationalen Cybersicherheitsstrategien auf die besonderen Cybersicherheitsbedürfnisse von kleinen und mittleren Unternehmen eingehen. Kleine und mittlere Unternehmen stellen in der gesamten Union einen großen Prozentsatz des Industrie-/Geschäftsmarktes und haben damit zu kämpfen, sich an ein neues Geschäftsgebaren in einer stärker vernetzten Welt anzupassen und sich in der digitalen Umgebung zurechtzufinden, in der Mitarbeiter von zu Hause aus arbeiten und Geschäfte zunehmend online getätigt werden. Einige kleine und mittlere Unternehmen stehen vor besonderen Herausforderungen im Bereich der Cybersicherheit, wie z. B. geringes Cyberbewusstsein, fehlende IT-Sicherheit aus der Ferne, hohe Kosten für Cybersicherheitslösungen und ein erhöhtes Maß an Bedrohungen, wie z. B. Ransomware, für die sie Anleitung und Unterstützung erhalten sollten. Kleine und mittlere Unternehmen werden aufgrund ihrer weniger strengen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und ihres geringer ausgeprägten Angriffsmanagements sowie der Tatsache, dass sie

über eingeschränkte Sicherheitsressourcen verfügen, zunehmend zum Ziel von Angriffen auf die Lieferkette. Diese Angriffe auf die Lieferkette wirken sich nicht nur auf kleine und mittlere Unternehmen und deren eigene Geschäftstätigkeit aus, sondern können im Rahmen größerer Angriffe auch eine Kaskadenwirkung auf die von ihnen belieferten Einrichtungen haben. Die Mitgliedstaaten sollten mittels ihrer nationalen Cybersicherheitsstrategien kleine und mittlere Unternehmen dabei unterstützen, die Herausforderungen in ihren Lieferketten zu bewältigen. Die Mitgliedstaaten sollten über eine Kontaktstelle für kleine und mittlere Unternehmen auf nationaler oder regionaler Ebene verfügen, die kleinen und mittleren Unternehmen entweder Leitlinien und Unterstützung bietet oder sie an die geeigneten Stellen für Leitlinien und Unterstützung in Fragen im Zusammenhang mit der Cybersicherheit weiterleitet. Die Mitgliedstaaten werden außerdem angehalten, auch Kleinstunternehmen und kleinen Unternehmen, die nicht über diese Fähigkeiten verfügen, Dienste wie die Konfiguration von Websites und die Aktivierung der Protokollierung anzubieten.

(57) Im Rahmen ihrer nationalen Cybersicherheitsstrategien sollten die Mitgliedstaaten Maßnahmen zur Förderung eines aktiven Cyberschutzes ergreifen. Anstatt nur zu reagieren, besteht aktiver Cyberschutz in der aktiven Verhütung, Erkennung, Überwachung, Analyse und Abschwächung von Sicherheitsverletzungen im Netzwerk, kombiniert mit der Nutzung von Kapazitäten, die innerhalb und außerhalb des Opfernetzwerks eingesetzt werden. Dies könnte auch die Bereitstellung kostenfreier Dienste oder Instrumente für bestimmte Einrichtungen, einschließlich Selbstbedienungskontrollen (self-service checks), Detektionswerkzeugen und Bereinigungsdiensten, durch die Mitgliedstaaten einschließen. Die Fähigkeit, Bedrohungsinformationen und -analysen, Warnungen zu Cyberaktivitäten und Reaktionsmaßnahmen schnell und automatisch auszutauschen und zu verstehen, ist entscheidend, um eine einheitliche Vorgehensweise bei der erfolgreichen Verhütung, Erkennung, Bekämpfung und Blockierung von Angriffen gegen Netz- und Informationssysteme zu ermöglichen. Der aktive Cyberschutz beruht auf einer defensiven Strategie, die offensive Maßnahmen ausschließt.

(58) Da durch die Ausnutzung von Schwachstellen in Netz- und Informationssystemen erhebliche Störungen und Schäden verursacht werden können, ist die rasche Erkennung und Behebung dieser Schwachstellen ein wichtiger Faktor bei der Verringerung des Risikos. Einrichtungen, die Netz- und Informationssysteme entwickeln oder verwalten, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten oder meldenden Einrichtungen entdeckt und offengelegt werden, sollte der Hersteller oder Anbieter von IKT-Produkten oder -Diensten auch Verfahren einführen, damit er von Dritten Informationen über Schwachstellen entgegennehmen kann. Diesbezüglich enthalten die internationalen Normen ISO/IEC 30111 und ISO/IEC 29147 Leitlinien für die Behandlung von Schwachstellen und die Offenlegung von Schwachstellen. Eine stärkere Koordinierung zwischen meldenden natürlichen und juristischen Personen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten ist besonders wichtig, um den freiwilligen Rahmen für die Offenlegung von Schwachstellen attraktiver zu machen. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder -Dienste Schwachstellen in einer Weise gemeldet werden, die ihm die Diagnose und Behebung der Schwachstelle ermöglicht, bevor detaillierte Informationen über die Schwachstelle an Dritte oder die Öffentlichkeit weitergegeben werden. Die koordinierte Offenlegung von Schwachstellen sollte auch die Koordinierung zwischen der meldenden natürlichen oder juristischen Person und dem Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder -Dienste in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

(59) Die Kommission, die ENISA und die Mitgliedstaaten sollten die Anpassung an internationale Normen und vorliegende bewährte Verfahren der Branche beim Risikomanagement im Bereich der Cybersicherheit weiterhin fördern, beispielsweise in den Bereichen Bewertungen der Sicherheit der Lieferkette, Informationsaustausch und Offenlegung von Schwachstellen.

(60) Die Mitgliedstaaten sollten in Zusammenarbeit mit der ENISA Maßnahmen ergreifen, um eine koordinierte Offenlegung von Schwachstellen zu erleichtern, indem sie eine einschlägige nationale Strategie festlegen. Die Mitgliedstaaten sollten im Rahmen ihrer nationalen Strategien im Einklang mit den nationalen Rechtsvorschriften so weit wie möglich die Herausforderungen angehen, mit denen Forscher, die sich mit Schwachstellen befassen, konfrontiert sind, wozu auch deren potenzielle strafrechtliche Haftung gehört. Da natürliche und juristische Personen, die Schwachstellen erforschen, in einigen Mitgliedstaaten der strafrechtlichen und zivilrechtlichen Haftung unterliegen könnten, werden die Mitgliedstaaten aufgefordert, Leitlinien für die Nichtverfolgung von Forschern im Bereich der Informationssicherheit zu verabschieden und eine Ausnahme von der zivilrechtlichen Haftung für ihre Tätigkeiten zu erlassen.

(61) Die Mitgliedstaaten sollten eines ihrer CSIRTs als Koordinator benennen, der gegebenenfalls als vertrauenswürdiger Vermittler zwischen den meldenden natürlichen oder juristischen Personen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten, die wahrscheinlich von der Schwachstelle betroffen sind, fungiert. Zu den Aufgaben des als Koordinator benannten CSIRT sollte insbesondere gehören, betreffende Einrichtungen zu ermitteln und zu

kontaktieren, die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen, Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen (koordinierte Offenlegung von Schwachstellen, die mehrere Parteien betreffen). Könnte die gemeldete Schwachstelle in mehr als einem Mitgliedstaat erhebliche Auswirkungen auf Einrichtungen haben, sollten die als Koordinator benannten CSIRTs gegebenenfalls im Rahmen des CSIRTs-Netzwerks zusammenarbeiten.

(62) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. Öffentlich zugängliche Informationen über Schwachstellen sind nicht nur für die Einrichtungen und die Nutzer ihrer Dienste, sondern auch für die zuständigen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA eine europäische Schwachstellendatenbank einrichten, in der Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, und deren Anbieter von Netz- und Informationssystemen sowie die zuständigen Behörden und CSIRTs auf freiwilliger Basis öffentlich bekannte Schwachstellen offenlegen und registrieren können, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen. Das Ziel dieser Datenbank besteht darin, die einzigartigen Herausforderungen zu bewältigen, die sich aus den Risiken für Einrichtungen der Union ergeben. Darüber hinaus sollte die ENISA ein geeignetes Verfahren für den Veröffentlichungsprozess einführen, um den Einrichtungen Zeit zu geben, Maßnahmen zur Behebung ihrer Schwachstellen zu ergreifen und moderne Risikomanagementmaßnahmen im Bereich der Cybersicherheit sowie maschinenlesbare Datensätze und entsprechende Schnittstellen einzusetzen. Zur Förderung einer Kultur der Offenlegung von Schwachstellen sollte eine Offenlegung ohne nachteilige Folgen für die meldende natürliche oder juristische Person erfolgen.

(63) Es gibt zwar bereits ähnliche Register oder Datenbanken für Schwachstellen, aber diese werden von Einrichtungen betrieben und gepflegt, die nicht in der Union niedergelassen sind. Eine von der ENISA gepflegte europäische Schwachstellendatenbank würde für mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der öffentlichen Offenlegung der Schwachstelle sorgen und die Resilienz im Falle von einer Störung oder Unterbrechung bei der Erbringung ähnlicher Dienste verbessern. Um Doppelarbeit so weit wie möglich zu vermeiden und im Interesse der größtmöglichen Komplementarität, sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ähnlichen Registern oder Datenbanken zu schließen, die unter die Gerichtsbarkeit von Drittländern fallen. Insbesondere sollte die ENISA die Möglichkeit einer engen Zusammenarbeit mit den Betreibern des Systems für bekannte Schwachstellen und Anfälligkeiten (CVE) prüfen.

(64) Die Kooperationsgruppe sollte die strategische Zusammenarbeit und den Informationsaustausch unterstützen und erleichtern und das Vertrauen zwischen den Mitgliedstaaten stärken. Die Kooperationsgruppe sollte alle zwei Jahre ein Arbeitsprogramm aufstellen. In dem Arbeitsprogramm sollten die Maßnahmen aufgeführt sein, die die Kooperationsgruppe zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen hat. Der Zeitrahmen für die Aufstellung des Arbeitsprogramms gemäß der vorliegenden Richtlinie sollte an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 aufgestellten Arbeitsprogramms angepasst werden, um etwaige Unterbrechungen der Arbeit der Kooperationsgruppe zu vermeiden.

(65) Bei der Ausarbeitung von Leitfäden sollte die Kooperationsgruppe konsequent nationale Lösungen und Erfahrungen erfassen, die Auswirkungen ihrer Vorgaben auf nationale Ansätze bewerten, Herausforderungen bei der Umsetzung erörtern und spezifische Empfehlungen für eine bessere Umsetzung bestehender Vorschriften formulieren, insbesondere hinsichtlich der Erleichterung der Angleichung bei der Umsetzung dieser Richtlinie zwischen den Mitgliedstaaten. Die Kooperationsgruppe könnte auch eine Bestandsaufnahme der nationalen Lösungen vornehmen, um die Kompatibilität von Cybersicherheitslösungen zu fördern, die für jeden einzelnen Sektor in der gesamten Union angewandt werden. Dies gilt insbesondere für Sektoren mit internationalem oder grenzüberschreitendem Charakter.

(66) Die Kooperationsgruppe sollte ein flexibles Forum bleiben und in der Lage sein, unter Berücksichtigung der verfügbaren Ressourcen auf sich ändernde und neue politische Prioritäten und Herausforderungen zu reagieren. Sie könnte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Kooperationsgruppe zu erörtern und Daten und Beiträge zu neuen politischen Herausforderungen einzuholen. Darüber hinaus sollte die Kooperationsgruppe regelmäßig den aktuellen Stand in Bezug auf Cyberbedrohungen oder -vorfälle wie Ransomware bewerten. Um die Zusammenarbeit auf Unionsebene

zu verbessern, sollte die Kooperationsgruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste einschlägige Organe, Einrichtungen und Agenturen der Union, etwa das Europäische Parlament, Europol, den Europäischen Datenschutzausschuss, die Agentur der Europäischen Union für Flugsicherheit, die mit der Verordnung (EU) 2018/1139 eingerichtet wurde, und die Agentur der Europäischen Union für das Weltraumprogramm, die mit der Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates ([14]) eingeführt wurde, zur Teilnahme an ihrer Arbeit einzuladen.

(67) Die zuständigen Behörden und die CSIRTs sollten die Möglichkeit haben, innerhalb eines spezifischen Rahmens und gegebenenfalls vorbehaltlich der erforderlichen Sicherheitsüberprüfung der an solchen Austauschprogrammen teilnehmenden Beamten an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern und das Vertrauen unter den Mitgliedstaaten zu stärken. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde oder des aufnehmenden CSIRT konstruktiv mitwirken können.

(68) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke — insbesondere dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe), das CSIRTs-Netzwerk und die Kooperationsgruppe — zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 der Kommission ([15]) beitragen. EU-CyCLONe und das CSIRTs-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Einzelheiten dieser Zusammenarbeit festgelegt werden, und jegliche Doppelarbeit vermeiden. In der Geschäftsordnung von EU-CyCLONe sollten die Regelungen für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich der Funktion und Aufgaben des Netzwerks, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf Unionsebene sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen gemäß dem Durchführungsbeschluss (EU) 2018/1993 des Rates ([16]) (IPCR-Regelung) stützen. Die Kommission sollte zu diesem Zweck auf den sektorübergreifenden Krisenkoordinierungsprozess auf hoher Ebene, ARGUS, zurückgreifen. Berührt die Krise eine wichtige externe Dimension oder eine Dimension der Gemeinsamen Sicherheits- und Verteidigungspolitik, so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes ausgelöst werden.

(69) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1584 sollte der Begriff „Cybersicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat. Je nach Ursache und Auswirkung können sich Cybersicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern oder ernsthafte, die öffentliche Sicherheit betreffende Risiken für Einrichtungen und Bürger in mehreren Mitgliedstaaten oder in der gesamten Union darstellen. Angesichts der großen Tragweite und des, in den meisten Fällen, grenzübergreifenden Charakters solcher Sicherheitsvorfälle sollten die Mitgliedstaaten und die einschlägigen Organe, Einrichtungen und sonstigen Stellen der Union auf technischer, operativer und politischer Ebene zusammenarbeiten, um die Reaktion unionsweit angemessen zu koordinieren.

(70) Cybersicherheitsvorfälle großen Ausmaßes und Krisen auf Unionsebene erfordern aufgrund der starken Interdependenz zwischen Sektoren und Mitgliedstaaten ein koordiniertes Vorgehen, um eine schnelle und wirksame Reaktion zu gewährleisten. Die Verfügbarkeit von gegen Cyberangriffe widerstandsfähigen Netz- und Informationssystemen sowie die Verfügbarkeit, Vertraulichkeit und Integrität von Daten sind von entscheidender Bedeutung für die Sicherheit der Union und den Schutz ihrer Bürger, Unternehmen und Institutionen vor Sicherheitsvorfällen und Cyberbedrohungen sowie für die Stärkung des Vertrauens von Einzelpersonen und Organisationen in die Fähigkeit der Union, einen globalen, offenen, freien, stabilen und sicheren Cyberraum zu fördern und zu schützen, der auf Menschenrechten, Grundfreiheiten, Demokratie und Rechtsstaatlichkeit beruht.

([14]) Verordnung (EU) 2021/696 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung des Weltraumprogramms der Union und der Agentur der Europäischen Union für das Weltraumprogramm und zur Aufhebung der Verordnungen (EU) Nr. 912/2010, (EU) Nr. 1285/2013 und (EU) Nr. 377/2014 sowie des Beschlusses Nr. 541/2014/EU (ABl. L 170 vom 12.5.2021, S. 69).

([15]) Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

([16]) Durchführungsbeschluss (EU) 2018/1993 des Rates vom 11. Dezember 2018 über die integrierte EU-Regelung für die politische Reaktion auf Krisen (ABl. L 320 vom 17.12.2018, S. 28).

(71) Das EU-CyCLONe sollte im Fall von Cybersicherheitsvorfällen großen Ausmaßes und Krisen als Vermittler zwischen der technischen und politischen Ebene fungieren und die Zusammenarbeit auf operativer Ebene verbessern und die Entscheidungsfindung auf politischer Ebene unterstützen. In Zusammenarbeit mit der Kommission und unter Berücksichtigung der Zuständigkeiten der Kommission im Bereich des Krisenmanagements sollte das EU-CyCLONe auf den Erkenntnissen des CSIRTs-Netzwerks aufbauen und seine eigenen Fähigkeiten nutzen, um Folgenabschätzungen für Cybersicherheitsvorfälle großen Ausmaßes und Krisen zu erstellen.

(72) Cyberangriffe sind grenzüberschreitender Natur, und ein erheblicher Sicherheitsvorfall kann kritische Informationsinfrastrukturen, von denen das reibungslose Funktionieren des Binnenmarkts abhängt, stören und schädigen. In der Empfehlung (EU) 2017/1584 wird auf die Rolle aller relevanten Akteure eingegangen. Darüber hinaus ist die Kommission im Rahmen des durch den Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates ([17]) eingerichteten Katastrophenschutzverfahrens der Union für allgemeine Vorsorgemaßnahmen zuständig, einschließlich der Verwaltung des Zentrums für die Koordination von Notfallmaßnahmen und des Gemeinsamen Kommunikations- und Informationssystems für Notfälle, der Aufrechterhaltung und Weiterentwicklung der Fähigkeit zur Lageerfassung und -analyse sowie des Aufbaus und der Verwaltung der Fähigkeit zur Mobilisierung und Entsendung von Expertenteams im Falle eines Hilfeersuchens eines Mitgliedstaats oder eines Drittstaats. Die Kommission ist auch für die Erstellung von Analyseberichten für die IPCR-Regelung gemäß dem Durchführungsbeschluss (EU) 2018/1993 zuständig, unter anderem in Bezug auf die Lageerfassung und -vorsorge im Bereich der Cybersicherheit sowie für die Lageerfassung und Krisenreaktion in den Bereichen Landwirtschaft, widrige Witterungsbedingungen, Konfliktkartierung und -vorhersagen, Frühwarnsysteme für Naturkatastrophen, gesundheitliche Notlagen, Überwachung von Infektionskrankheiten, Pflanzengesundheit, chemische Zwischenfälle, Lebensmittel- und Futtermittelsicherheit, Tiergesundheit, Migration, Zoll, Notlagen im Bereich Kernenergie und Strahlenforschung, und Energie.

(73) 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 EU-CyCLONe ermöglicht und geregelt wird. Solche Übereinkünfte sollten die Interessen der Union wahren und einen angemessenen Datenschutz gewährleisten. Das sollte nicht das Recht der Mitgliedstaaten ausschließen, mit Drittländern bei der Verwaltung von Schwachstellen und von Cybersicherheitsrisiken zusammenzuarbeiten und die Berichterstattung und den allgemeinen Informationsaustausch im Einklang mit dem Recht der Union zu erleichtern.

(74) Um die wirksame Umsetzung der Bestimmungen dieser Richtlinie, etwa zum Umgang mit Schwachstellen, zu Risikomanagementmaßnahmen im Bereich der Cybersicherheit, zu Berichtspflichten und zu Vereinbarungen über den Austausch cyberbezogener Informationen, zu fördern, können die Mitgliedstaaten mit Drittländern zusammenarbeiten und Tätigkeiten durchführen, die für diesen Zweck als angemessen erachtet werden, wozu auch der Informationsaustausch über Cyberbedrohungen, Vorfälle, Schwachstellen, Instrumente und Methoden, Taktiken, Techniken und Verfahren, die Vorsorge und Übungen im Hinblick auf das Krisenmanagement im Cyberbereich, Schulungen, die Vertrauensbildung und Vereinbarungen über den strukturierten Informationsaustausch gehören.

(75) Peer Reviews sollten eingeführt werden, um aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu stärken und ein hohes gemeinsames Cybersicherheitsniveau zu erreichen. Peer Reviews können zu wertvollen Erkenntnissen und Empfehlungen führen, mit denen man die allgemeinen Cybersicherheitskapazitäten stärkt, einen weiteren funktionalen Weg für den Austausch bewährter Verfahren zwischen den Mitgliedstaaten schafft und dazu beiträgt, den Reifegrad der Mitgliedstaaten im Bereich der Cybersicherheit zu verbessern. Darüber hinaus sollte bei den Peer Reviews den Ergebnissen ähnlicher Mechanismen, wie dem Peer-Review-System des CSIRTs-Netzwerks, Rechnung getragen, ein Mehrwert geschaffen und Doppelarbeit vermieden werden. Die Umsetzung der Peer Reviews sollte die Rechtsvorschriften der Union und der Mitgliedstaaten über den Schutz vertraulicher oder als Verschlusssachen eingestufter Informationen unberührt lassen.

(76) Die Kooperationsgruppe sollte eine Selbstbewertungsmethode für die Mitgliedstaaten festlegen, die Faktoren wie den Stand der Umsetzung der Maßnahmen für das Cybersicherheitsrisikomanagement und die Berichtspflichten, den Umfang der Fähigkeiten und die Wirksamkeit der Wahrnehmung der Aufgaben der zuständigen Behörden, die operativen Fähigkeiten der CSIRTs, den Grad der Umsetzung der Amtshilfe sowie der Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder spezifische Fragen grenz- oder sektorübergreifender Art abdeckt. Die Mitgliedstaaten sollten angehalten werden, regelmäßig Selbstbewertungen durchzuführen und die Ergebnisse ihrer Selbstbewertung in der Kooperationsgruppe vorzustellen und zu erörtern.

([17]) Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates vom 17. Dezember 2013 über ein Katastrophenschutzverfahren der Union (ABl. L 347 vom 20.12.2013, S. 924).

(77) Die Verantwortung für die Gewährleistung der Sicherheit von Netz- und Informationssystemen liegt in erheblichem Maße bei den wesentlichen und wichtigen Einrichtungen. Es sollte eine Risikomanagementkultur gefördert und entwickelt werden, die unter anderem die Risikobewertung und die Anwendung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die den jeweiligen Risiken angemessen sind, umfassen sollte.

(78) Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten den Grad der Abhängigkeit der wesentlichen oder wichtigen Einrichtung von Netz- und Informationssystemen berücksichtigen und auch Maßnahmen zur Ermittlung jeder Gefahr eines Sicherheitsvorfalls, zur Verhinderung, und Aufdeckung von Sicherheitsvorfällen, zur Reaktion darauf und zur Wiederherstellung danach sowie der Minderung ihrer Folgen umfassen. Die Sicherheit von Netz- und Informationssystemen sollte sich auch auf gespeicherte, übermittelte und verarbeitete Daten erstrecken. Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten eine systemische Analyse vorsehen, bei der der menschliche Faktor berücksichtigt wird, um ein vollständiges Bild der Sicherheit des Netz- und Informationssystems zu erhalten.

(79) Da Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, sollten Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, Netz- und Informationssysteme und ihr physisches Umfeld vor Ereignissen wie Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen oder vor unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen einer wesentlichen oder wichtigen Einrichtung und vor der Schädigung dieser Informationen und Anlagen und den entsprechenden Eingriffen zu schützen, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können. Bei den Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten daher auch die physische Sicherheit und die Sicherheit des Umfelds von Netz- und Informationssystemen berücksichtigt werden, indem Maßnahmen zum Schutz dieser Systeme vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen im Einklang mit europäischen und internationalen Normen, wie denen der Reihe ISO/IEC 27000, einbezogen werden. In diesem Zusammenhang sollten sich die wesentlichen und wichtigen Einrichtungen im Rahmen ihrer Risikomanagementmaßnahmen im Bereich der Cybersicherheit auch mit der Sicherheit des Personals befassen und über angemessene Konzepte für die Zugangskontrolle verfügen. Diese Maßnahmen sollten mit der Richtlinie (EU) 2022/2557 im Einklang stehen.

(80) Zum Nachweis der Einhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit und in Ermangelung gemäß der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([18]) verabschiedeter geeigneter europäischer Schemata für die Cybersicherheitszertifizierung sollten die Mitgliedstaaten nach Konsultation der Kooperationsgruppe und der Europäischen Gruppe für die Cybersicherheitszertifizierung die Anwendung einschlägiger europäischer und internationaler Normen durch wesentliche und wichtige Einrichtungen fördern oder Einrichtungen zur Verwendung zertifizierter IKT-Produkte, -Dienste und -Verfahren verpflichten.

(81) Damit keine unverhältnismäßige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Risikomanagementmaßnahmen im Bereich der Cybersicherheit in einem angemessenen Verhältnis zu den Risiken stehen, denen das betreffende Netz- und Informationssystem ausgesetzt ist; dabei wird dem bei solchen Maßnahmen geltenden neuesten Stand und gegebenenfalls europäischen oder internationalen Normen sowie den Kosten ihrer Umsetzung Rechnung getragen.

(82) Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sollten in einem angemessenen Verhältnis zum Grad der Risikoexposition der wesentlichen oder wichtigen Einrichtung und zu den gesellschaftlichen und wirtschaftlichen Auswirkungen stehen, die ein Sicherheitsvorfall hätte. Bei der Festlegung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, die an wesentliche und wichtige Einrichtungen angepasst sind, sollte der unterschiedlichen Risikoexposition wesentlicher und wichtiger Einrichtungen gebührend Rechnung getragen werden, wie z. B. der Kritikalität der Einrichtung, den Risiken, einschließlich der gesellschaftlichen Risiken, denen sie ausgesetzt ist, der Größe der Einrichtung, der Wahrscheinlichkeit des Auftretens von Sicherheitsvorfällen und ihrer Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen.

([18]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

(83) Wesentliche und wichtige Einrichtungen sollten die Sicherheit der bei ihren Tätigkeiten verwendeten Netz- und Informationssysteme gewährleisten. Hauptsächlich handelt es sich bei diesen Systemen um private Netz- und Informationssysteme, die entweder von internem IT-Personal der wesentlichen und wichtigen Einrichtung verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Anforderungen an die Risikomanagementmaßnahmen und die Berichtspflichten im Bereich der Cybersicherheit gemäß der vorliegenden Richtlinie sollten für die einschlägigen wesentlichen und wichtigen Einrichtungen unabhängig davon gelten, ob diese Einrichtungen ihre Netz- und Informationssysteme intern warten oder deren Wartung ausgliedern.

(84) Angesichts der grenzüberschreitenden Art ihrer Tätigkeit sollte bei DNS-Diensteanbietern, TLD-Namenregistern, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Anbietern verwalteter Dienste und Anbietern verwalteter Sicherheitsdienste, Anbietern von Online-Marktplätzen, von Online-Suchmaschinen und von Plattformen für Dienste sozialer Netzwerke und Anbietern von Vertrauensdiensten auf Unionsebene eine stärkere Harmonisierung erfolgen. Die Umsetzung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit hinsichtlich dieser Einrichtungen sollte daher durch einen Durchführungsrechtsakt erleichtert werden.

(85) Besonders wichtig ist die Bewältigung von Risiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten, z. B. Anbietern von Datenspeicherungs- und -verarbeitungsdiensten oder Anbietern von verwalteten Sicherheitsdiensten und Softwareherstellern, betreffen, da sich die Vorfälle häufen, bei denen Einrichtungen Opfer von Cyberangriffen werden und es böswilligen Akteuren gelingt, die Sicherheit der Netz- und Informationssysteme zu beeinträchtigen, indem Schwachstellen im Zusammenhang mit den Produkten und Diensten Dritter ausgenutzt werden. Die wesentlichen und wichtigen Einrichtungen sollten daher die Gesamtqualität und Widerstandsfähigkeit der Produkte und Diensten, die darin enthaltenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit und die Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen. Die wesentlichen und wichtigen Einrichtungen sollten insbesondere dazu angehalten werden, Risikomanagementmaßnahmen im Bereich der Cybersicherheit in die vertraglichen Vereinbarungen mit ihren direkten Lieferanten und Diensteanbietern Ebene einzubeziehen. Diese Einrichtungen könnten auch die Risiken berücksichtigen, die von Lieferanten und Dienstleistern anderer Ebenen ausgehen.

(86) Unter den Diensteanbietern spielen die Anbieter verwalteter Sicherheitsdienste in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen sowie die Wiederherstellung danach unterstützen. Allerdings sind auch die Anbieter verwalteter Sicherheitsdienste selbst das Ziel von Cyberangriffen und stellen aufgrund ihrer engen Einbindung in die Tätigkeiten von wesentlichen und wichtigen Einrichtungen ein besonderes Risiko dar. Die Einrichtungen sollten daher bei der Wahl eines Anbieters verwalteter Sicherheitsdienste erhöhte Sorgfalt walten lassen.

(87) Die zuständigen Behörden können im Rahmen ihrer Aufsichtsaufgaben auch Cybersicherheitsdienste für beispielsweise Sicherheitsprüfungen und Penetrationstests oder die Reaktion auf Sicherheitsvorfälle nutzen.

(88) Die wesentlichen und wichtigen Einrichtungen sollten sich auch mit Risiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben, unter anderem im Hinblick auf die Abwehr von Wirtschaftsspionage und den Schutz von Geschäftsgeheimnissen. Insbesondere sollten diese Einrichtungen durch geeignete Maßnahmen sicherstellen, dass ihre Zusammenarbeit mit Hochschul- und Forschungseinrichtungen ihrer Cybersicherheitsstrategie entspricht und dabei bewährte Verfahren befolgt werden, was den sicheren Zugang zu sowie die Verbreitung von Informationen im Allgemeinen und den Schutz des geistigen Eigentums im Besonderen angeht. Auch sollten in Anbetracht der Bedeutung und des Wertes von Daten für die Tätigkeiten der wesentlichen und wichtigen Einrichtungen letztere alle geeigneten Risikomanagementmaßnahmen im Bereich der Cybersicherheit ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.

(89) Die wesentlichen und wichtigen Einrichtungen sollten eine breite Palette grundlegender Praktiken der Cyberhygiene anwenden, z. B. Zero-Trust-Grundsätze, Software-Updates, Gerätekonfiguration, Netzwerksegmentierung, Identitäts- und Zugriffsmanagement oder Sensibilisierung der Nutzer, Schulungen für ihre Mitarbeiter organisieren und das Bewusstsein für Cyberbedrohungen, Phishing oder Social-Engineering-Techniken schärfen. Außerdem sollten diese Einrichtungen ihre eigenen Cybersicherheitskapazitäten bewerten und gegebenenfalls die Integration von Technologien zur Verbesserung der Cybersicherheit anstreben, etwa künstliche Intelligenz oder Systeme des maschinellen Lernens, um ihre Kapazitäten und die Sicherheit von Netz- und Informationssystemen zu erhöhen.

(90) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den wesentlichen und wichtigen Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Risiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe in Zusammenarbeit mit der Kommission und der ENISA und gegebenenfalls nach Konsultation der einschlägigen Interessenträger, auch aus der Wirtschaft koordinierte Risikobewertungen kritischer Lieferketten — wie im Fall der 5G-Netze gemäß der Empfehlung (EU) 2019/534 der Kommission ([19]) — durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln. Bei solchen koordinierten Risikobewertungen sollten Maßnahmen, Pläne zur Risikominderung und bewährte Verfahren gegen kritische Abhängigkeiten, potenzielle einzelne Fehlerquellen, Bedrohungen, Schwachstellen und andere Risiken im Zusammenhang mit der Lieferkette ermittelt werden, und es sollte nach Möglichkeiten gesucht werden, ihre breitere Anwendung durch die wesentlichen und wichtigen Einrichtungen zu fördern. Zu den potenziellen nichttechnischen Risikofaktoren wie ungebührlicher Einflussnahme eines Drittlandes auf Lieferanten und Diensteanbieter, insbesondere im Fall von alternativen Governance-Modellen, zählen versteckte Schwachstellen oder Hintertüren sowie potenzielle systemische Versorgungsunterbrechungen, insbesondere im Fall von Abhängigkeiten von bestimmten Technologien oder Anbietern.

(91) Bei den koordinierten Risikobewertungen kritischer Lieferketten unter Berücksichtigung der Besonderheiten des jeweiligen Sektors sollte sowohl technischen wie auch gegebenenfalls nichttechnischen Faktoren Rechnung getragen werden, einschließlich derer, die in der Empfehlung (EU) 2019/534, in der koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen der EU sowie in dem von der Kooperationsgruppe vereinbarten EU-Instrumentarium für die 5G-Cybersicherheit definiert sind. Bei der Ermittlung der Lieferketten, die einer koordinierten Risikobewertung unterzogen werden sollten, sollten folgende Kriterien berücksichtigt werden: i) der Umfang, in dem wesentliche und wichtige Einrichtungen bestimmte kritische IKT-Dienste, -Systeme oder -Produkte nutzen und auf sie angewiesen sind; ii) die Bedeutung bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte für die Ausführung kritischer oder sensibler Funktionen, einschließlich der Verarbeitung personenbezogener Daten; iii) die Verfügbarkeit alternativer IKT-Dienste, -Systeme oder -Produkte; iv) die Resilienz der gesamten Lieferkette von IKT-Diensten, -Systemen oder -Produkten während ihres gesamten Lebenszyklus gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen. Besonderes Augenmerk sollte auf IKT-Diensten, -Systeme oder -Produkte gelegt werden, die speziellen Anforderungen unterliegen, die von Drittländern stammen.

(92) Zur Straffung der Verpflichtungen, die Anbietern öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste sowie Vertrauensdiensteanbietern hinsichtlich der Sicherheit ihrer Netz- und Informationssysteme auferlegt werden, und um diese Einrichtungen und die zuständigen Behörden nach der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([20]) bzw. der Verordnung (EU) Nr. 910/2014 von dem durch diese Richtlinie geschaffenen Rechtsrahmen profitieren zu lassen, einschließlich der Benennung der für die Bewältigung von Sicherheitsvorfällen zuständigen Computer-Notfallteams (CSIRTs), Beteiligung der betreffenden zuständigen Behörden an den Tätigkeiten der Kooperationsgruppe und des CSIRTs-Netzwerks, sollten diese Einrichtungen in den Anwendungsbereich dieser Richtlinie fallen. Die entsprechenden Bestimmungen der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972, mit denen diesen Arten von Einrichtungen Sicherheitsanforderungen und Berichtspflichten auferlegt werden, sollten daher gestrichen werden. Die Vorschriften über die Berichtspflichten gemäß der vorliegenden Richtlinie sollten die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG unberührt lassen.

(93) Die in dieser Richtlinie festgelegten Cybersicherheitspflichten sollten als Ergänzung zu den Anforderungen betrachtet werden, denen die Vertrauensdiensteanbieter gemäß der Verordnung (EU) Nr. 910/2014 unterliegen. Vertrauensdiensteanbieter sollten verpflichtet werden, alle geeigneten und verhältnismäßigen Maßnahmen zu ergreifen, um die sich für ihre Dienste, aber auch ihre Kunden und vertrauende Dritte ergebenden Risiken zu beherrschen und Sicherheitsvorfälle gemäß dieser Richtlinie zu melden. Diese Cybersicherheits- und Berichtspflichten sollten auch den physischen Schutz der angebotenen Dienste betreffen. Die Anforderungen an qualifizierte Vertrauensdiensteanbieter gemäß Artikel 24 der Verordnung (EU) Nr. 910/2014 gelten weiterhin.

([19]) Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze (ABl. L 88 vom 29.3.2019, S. 42).

([20]) Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (ABl. L 321 vom 17.12.2018, S. 36).

(94) Die Mitgliedstaaten können den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014 die Funktion der für Vertrauensdienste zuständigen Behörden übertragen, um die Fortführung der derzeitigen Verfahrensweisen sicherzustellen und auf den Erkenntnissen und Erfahrungen aufzubauen, die bei der Anwendung dieser Verordnung gewonnen wurden. In diesem Fall sollten die nach dieser Richtlinie zuständigen Behörden eng und zeitnah mit diesen Aufsichtsstellen zusammenarbeiten, indem sie die einschlägigen Informationen austauschen, um eine wirksame Aufsicht und Einhaltung der Anforderungen dieser Richtlinie und der Verordnung (EU) Nr. 910/2014 durch die Vertrauensdiensteanbieter zu gewährleisten. Gegebenenfalls sollten das CSIRT oder die jeweilige nach dieser Richtlinie zuständige Behörde unverzüglich die Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014 über gemeldete erhebliche Cyberbedrohungen oder Vorfälle mit Auswirkungen auf Vertrauensdienste sowie über Verstöße gegen diese Richtlinie durch die Vertrauensdiensteanbieter unterrichten. Für die Zwecke der Meldung können die Mitgliedstaaten gegebenenfalls die zentrale Anlaufstelle nutzen, die eingerichtet wurde, um eine gemeinsame automatische Meldung von Vorfällen an die Aufsichtsstelle gemäß der Verordnung (EU) Nr. 910/2014 und das CSIRT oder die jeweilige nach dieser Richtlinie zuständige Behörde zu erreichen.

(95) Sofern angebracht und um unnötige Unterbrechungen zu vermeiden, sollten bestehende nationale Leitlinien, die zur Umsetzung der Vorschriften über Sicherheitsmaßnahmen gemäß den Artikeln 40 und 41 der Richtlinie (EU) 2018/1972 erlassen wurden, bei der Umsetzung dieser Richtlinie berücksichtigt werden, wobei auf den bereits im Rahmen der Richtlinie (EU) 2018/1972 erworbenen Kenntnissen und Fähigkeiten in Bezug auf Sicherheitsmaßnahmen und Meldungen von Zwischenfällen aufgebaut werden sollte. Zudem kann die ENISA Leitlinien zu den Sicherheitsanforderungen und Berichtspflichten für Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste ausarbeiten, damit die Harmonisierung und Umsetzung erleichtert und die Störungen auf ein Mindestmaß reduziert werden. Die Mitgliedstaaten können den nationalen Regulierungsbehörden die Funktion der für elektronische Kommunikation zuständigen Behörden gemäß der Richtlinie (EU) 2018/1972 übertragen, um die Fortführung der derzeitigen Verfahrensweisen sicherzustellen und auf den Erkenntnissen und Erfahrungen aufzubauen, die als Ergebnis der Anwendung jener Richtlinie gewonnen wurden.

(96) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972 muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Da sich die Angriffsfläche immer weiter vergrößert, werden nummernunabhängige interpersonelle Kommunikationsdienste, etwa Messenger-Dienste, zu weit verbreiteten Angriffsvektoren. Böswillige Akteure nutzen Plattformen, um zu kommunizieren und Opfer zum Öffnen kompromittierter Webseiten zu verleiten, wodurch sich die Wahrscheinlichkeit von Vorfällen erhöht, bei denen persönliche Daten verwertet und damit die Sicherheit von Netz- und Informationssystemen ausgenutzt wird. Die Anbieter von nummernunabhängigen interpersonellen Kommunikationsdiensten sollten daher auch ein Sicherheitsniveau von Netz- und Informationssystemen gewährleisten, das den bestehenden Risiken angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste im Sinne der Richtlinie (EU) 2018/1972 üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, können die Risiken für solche Dienste in gewisser Hinsicht als geringer erachtet werden als für herkömmliche elektronische Kommunikationsdienste. Dasselbe gilt auch für interpersonelle Kommunikationsdienste, die Nummern nutzen und die keine tatsächliche Kontrolle über die Signalübertragung ausüben.

(97) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienste fast aller wesentlichen und wichtigen Einrichtungen hängen ihrerseits von Diensten ab, die über das Internet erbracht werden. Für die reibungslose Bereitstellung von Diensten wesentlicher und wichtiger Einrichtungen ist es wichtig, dass alle Anbieter öffentlicher elektronischer Kommunikationsnetze über geeignete Risikomanagementmaßnahmen im Bereich der Cybersicherheit verfügen und diesbezügliche erhebliche Sicherheitsvorfälle melden. Die Mitgliedstaaten sollten dafür sorgen, dass die Sicherheit der öffentlichen elektronischen Kommunikationsnetze aufrechterhalten und ihre vitalen Sicherheitsinteressen vor Sabotage und Spionage geschützt werden. Da die internationale Konnektivität die wettbewerbsfähige Digitalisierung der Union und ihrer Wirtschaft verbessert und beschleunigt, sollten Sicherheitsvorfälle, die Unterseekommunikationskabel betreffen, dem CSIRT oder gegebenenfalls der zuständigen Behörde gemeldet werden. Die nationale Cybersicherheitsstrategie sollte gegebenenfalls der Cybersicherheit von Unterseekommunikationskabeln Rechnung tragen und eine Bestandsaufnahme potenzieller Cybersicherheitsrisiken und Risikominderungsmaßnahmen umfassen, um ein Höchstmaß an Schutz zu gewährleisten.

(98) Zur Aufrechterhaltung der Sicherheit öffentlicher elektronischer Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste sollte der Einsatz von Verschlüsselungstechnologien, insbesondere von Ende zu Ende, sowie datenzentrierter Sicherheitskonzepte wie Kartografie, Segmentierung, Kennzeichnung, Zugangspolitik und Zugangsverwaltung sowie automatisierte Zugangsentscheidungen gefördert werden. Erforderlichenfalls sollte der Einsatz von Verschlüsselung, insbesondere von Ende zu Ende, für die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke der vorliegenden Richtlinie vorgeschrieben werden. Die Nutzung der End-zu-End-Verschlüsselung sollte mit den Befugnissen der Mitgliedstaaten, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. Dies sollte jedoch nicht zu einer Schwächung der End-zu-End-Verschlüsselung führen, die eine entscheidende Technologie für einen wirksamen Datenschutz, einen entsprechenden Schutz der Privatsphäre und die Sicherheit der Kommunikation ist.

(99) Um die Sicherheit zu gewährleisten und den Missbrauch und die Manipulation elektronischer Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste zu verhindern, sollte die Verwendung interoperabler sicherer Routing-Standards gefördert werden, um die Integrität und Robustheit der Routing-Funktionen im gesamten Ökosystem der Anbieter von Internetzugangsdiensten sicherzustellen.

(100) Um die Funktionalität und Integrität des Internets zu wahren und die Sicherheit und Widerstandsfähigkeit des DNS zu stärken, sollten die einschlägigen Akteure, privatwirtschaftliche Einrichtungen der Union, Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, insbesondere Anbieter von Internetzugangsdiensten, und Anbieter von Online-Suchmaschinen, dazu angehalten werden, eine Strategie zur Diversifizierung der DNS-Auflösung zu verfolgen. Außerdem sollten die Mitgliedstaaten die Entwicklung und Nutzung eines öffentlichen und sicheren europäischen DNS-Auflösungsdienstes fördern.

(101) Mit dieser Richtlinie wird ein mehrstufiger Ansatz für die Meldung erheblicher Sicherheitsvorfälle festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung erheblicher Sicherheitsvorfälle entgegenwirkt und den wesentlichen und wichtigen Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Einrichtungen und ganze Sektoren ihre Cyberresilienz im Laufe der Zeit verbessern können. In diesem Zusammenhang sollte diese Richtlinie die Meldung von Sicherheitsvorfällen umfassen, die — auf der Grundlage einer von der betreffenden Einrichtung vorgenommenen Anfangsbewertung — erhebliche Betriebsstörungen des Dienstes oder finanzielle Verluste für diese Einrichtung verursachen oder andere natürliche oder juristische Personen betreffen könnten, indem sie erhebliche materielle oder immaterielle Schäden verursachen. Bei einer derartigen Anfangsbewertung sollten unter anderem die betroffenen Netz- und Informationssysteme und insbesondere deren Bedeutung für die Erbringung der Dienste der Einrichtung, die Schwere und die technischen Merkmale der Cyberbedrohung und alle zugrunde liegenden Schwachstellen, die ausgenutzt werden, sowie die Erfahrungen der Einrichtung mit ähnlichen Vorfällen berücksichtigt werden. Indikatoren wie das Ausmaß, in dem das Funktionieren des Dienstes beeinträchtigt wird, die Dauer eines Sicherheitsvorfalls oder die Zahl der betroffenen Nutzer von Diensten könnten eine wichtige Rolle bei der Feststellung spielen, ob die Betriebsstörung des Dienstes schwerwiegend ist.

(102) Erhalten wesentliche oder wichtige Einrichtungen Kenntnis von einem erheblichen Sicherheitsvorfall, sollten sie unverzüglich und spätestens binnen 24 Stunden eine Frühwarnung übermitteln müssen. Auf diese Frühwarnung sollte eine Meldung des Sicherheitsvorfalls folgen. Die betreffenden Einrichtungen sollten unverzüglich, in jedem Fall aber innerhalb von 72 Stunden, nachdem sie Kenntnis von dem erheblichen Sicherheitsvorfall erlangt haben, eine Meldung des Sicherheitsvorfalls übermitteln, um insbesondere die im Rahmen der Frühwarnung übermittelten Informationen zu aktualisieren und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seiner Schwere und seiner Auswirkungen, sowie etwaiger Kompromittierungsindikatoren (indicators of compromise — IoC), sofern verfügbar, vorzunehmen. Ein Abschlussbericht sollte spätestens einen Monat nach der Meldung des Sicherheitsvorfalls vorgelegt werden. Die Frühwarnung sollte lediglich die Informationen enthalten, die erforderlich sind, um das CSIRT oder gegebenenfalls die zuständige Behörde über den Sicherheitsvorfall zu unterrichten und es der betreffenden Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. In einer solchen Frühwarnung sollte gegebenenfalls angegeben werden, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall durch rechtswidrige oder böswillige Handlungen verursacht wurde, und ob er wahrscheinlich grenzüberschreitende Auswirkungen hat. Die Mitgliedstaaten sollten sicherstellen, dass die Verpflichtung, diese Frühwarnung oder die anschließende Meldung eines Sicherheitsvorfalls zu übermitteln, nicht dazu führt, dass die meldende Einrichtung die Ressourcen von Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen — was vorrangig

behandelt werden sollte — umlenken müssen, um zu verhindern, dass die Verpflichtung zur Meldung von Sicherheitsvorfällen entweder dazu führt, das Ressourcen für die Bewältigung erheblicher Sicherheitsvorfälle umgelenkt oder die diesbezüglichen Maßnahmen der Einrichtungen auf andere Weise beeinträchtigt werden. Im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts sollten die Mitgliedstaaten sicherstellen, dass die betreffenden Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des erheblichen Sicherheitsvorfalls vorlegen.

(103) Gegebenenfalls sollten die wesentlichen und wichtigen Einrichtungen den Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die sie ergreifen können, um die sich aus einer erheblichen Cyberbedrohung ergebenden Risiken zu mindern. Diese Einrichtungen sollten gegebenenfalls und insbesondere dann, wenn die erhebliche Cyberbedrohung wahrscheinlich eintreten wird, auch ihre Nutzer über die Bedrohung selbst informieren. Die Verpflichtung zur Information der Empfänger über solche erheblichen Bedrohungen sollte nach besten Kräften erfüllt werden, sollte diese Einrichtungen jedoch nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede derartige Bedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über erhebliche Cyberbedrohungen für die Empfänger sollte kostenlos sein, und die Informationen sollten in leicht verständlicher Sprache abgefasst werden.

(104) Die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste sollten Sicherheit durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen implementieren und die Empfänger der Dienste über erhebliche Cyberbedrohungen sowie über zusätzliche Maßnahmen zum Schutz ihrer Geräte und Kommunikationsinhalte, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.

(105) Ein proaktiver Ansatz gegen Cyberbedrohungen ist ein wesentlicher Bestandteil von Risikomanagement im Bereich der Cybersicherheit und sollte den zuständigen Behörden ermöglichen, wirksam zu verhindern, dass Cyberbedrohungen in Sicherheitsvorfälle münden, die erhebliche materielle oder immaterielle Schäden verursachen können. Zu diesem Zweck ist die Meldung von Cyberbedrohungen von zentraler Bedeutung. Zu diesem Zweck wird den Einrichtungen nahegelegt, Cyberbedrohungen auf freiwilliger Basis zu melden.

(106) Um die Übermittlung der nach dieser Richtlinie erforderlichen Informationen zu vereinfachen und den Verwaltungsaufwand für Einrichtungen zu verringern, sollten die Mitgliedstaaten technische Mittel wie eine zentrale Anlaufstelle, automatisierte Systeme, Online-Formulare, benutzerfreundliche Schnittstellen, Vorlagen, spezielle Plattformen für die Nutzung durch Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, für die Übermittlung der einschlägigen zu meldenden Informationen bereitstellen. Die Finanzierung durch die Union zur Unterstützung der Umsetzung dieser Richtlinie, insbesondere im Rahmen des mit der Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates ([21]) eingerichteten Programms „Digitales Europa", könnte die Unterstützung für zentrale Anlaufstellen umfassen. Einrichtungen sind darüber hinaus häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Berichtspflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichem Verwaltungsaufwand und könnten auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren führen. Wird eine zentrale Anlaufstelle eingerichtet, so wird den Mitgliedstaaten nahegelegt, diese zentrale Anlaufstelle auch für Meldungen von Sicherheitsvorfällen zu nutzen, die nach anderen Rechtsvorschriften der Union wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG erforderlich sind. Die Nutzung einer solchen zentralen Anlaufstelle für die Meldung von Sicherheitsvorfällen gemäß der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG sollte die Anwendung der Bestimmungen der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, insbesondere der Bestimmungen über die Unabhängigkeit der darin genannten Behörden, unberührt lassen. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster erstellen, um die Erteilung der gemäß dem Unionsrecht erforderlichen zu meldenden Informationen zu vereinfachen und zu straffen und den Verwaltungsaufwand für meldende Einrichtungen zu verringern.

(107) Wenn der Verdacht besteht, dass ein Sicherheitsvorfall im Zusammenhang mit schweren kriminellen Handlungen nach Unionsrecht oder nationalem Recht steht, sollten die Mitgliedstaaten wesentliche und wichtige Einrichtungen — auf der Grundlage geltender strafverfahrensrechtlicher Bestimmungen im Einklang mit dem Unionsrecht — dazu anhalten, diese Sicherheitsvorfälle mit einem mutmaßlichen schwerwiegenden kriminellen Hintergrund den zuständigen Strafverfolgungsbehörden zu melden. Unbeschadet der für Europol geltenden Vorschriften für den Schutz personenbezogener Daten ist gegebenenfalls die Unterstützung durch Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (EC3) und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.

([21]) Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Aufstellung des Programms „Digitales Europa" und zur Aufhebung des Beschlusses (EU) 2015/2240 (ABl. L 166 vom 11.5.2021, S. 1).

(108) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden mit den in der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG genannten Behörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

(109) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen-Registrierungsdaten („WHOIS-Daten“) und ein rechtmäßiger Zugang zu diesen Daten sind entscheidend, um die Sicherheit, Stabilität und Resilienz des DNS zu gewährleisten, was wiederum zu einem hohen gemeinsamen Cybersicherheitsniveau in der gesamten Union beiträgt. Zu diesem spezifischen Zweck sollten TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, verpflichtet sein, bestimmte Daten zu verarbeiten, die zur Erfüllung dieses Zwecks erforderlich sind. Die Verarbeitung stellt eine rechtliche Verpflichtung im Sinne von Artikel 6 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 dar. Diese Verpflichtung gilt unbeschadet der Möglichkeit, Domänennamen-Registrierungsdaten für andere Zwecke zu erheben, zum Beispiel auf der Grundlage vertraglicher Vereinbarungen oder rechtlicher Anforderungen, die in anderen Rechtsvorschriften der Union oder der Mitgliedstaaten festgelegt sind. Diese Verpflichtung zielt darauf ab, einen vollständigen und genauen Satz von Registrierungsdaten zu erreichen, und sollte nicht dazu führen, dass dieselben Daten mehrfach erhoben werden. Die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten zusammenarbeiten, um Doppelarbeit zu vermeiden.

(110) Die Verfügbarkeit und zeitnahe Zugänglichkeit von Domänennamen-Registrierungsdaten für berechtigte Zugangsnachfrager ist für die Prävention und Bekämpfung von DNS-Missbrauch sowie für die Prävention und Erkennung von Vorfällen und die Reaktion darauf von wesentlicher Bedeutung. Unter berechtigten Zugangsnachfragern ist jede natürliche oder juristische Person zu verstehen, die einen Antrag gemäß des Unionsrechts oder des nationalen Rechts stellt. Dazu gehören können nach dieser Richtlinie und nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten zuständige Behörden sowie CERTs oder CSIRTs. TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten verpflichtet sein, berechtigten Zugangsnachfragern im Einklang mit dem Unionsrecht und den nationalen Rechtsvorschriften rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten, die zum Zwecke des Antrags auf Zugang notwendig sind, zu gewähren. Dem Antrag berechtigter Zugangsnachfrager sollte eine Begründung beigefügt sein, die es ermöglicht, die Notwendigkeit des Zugangs zu den Daten zu beurteilen.

(111) Zur Gewährleistung der Verfügbarkeit genauer und vollständiger Domänennamen-Registrierungsdaten sollten die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste, die Integrität und Verfügbarkeit von Domänennamen-Registrierungsdaten erfassen und garantieren. Insbesondere sollten TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Grundsätze und Verfahren festlegen, um im Einklang mit dem Datenschutzrecht der Union genaue und vollständige Domänennamen-Registrierungsdaten zu erfassen und zu pflegen sowie unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen. Diese Strategien und Verfahren sollten so weit wie möglich den von den Multi-Stakeholder-Governance-Strukturen auf internationaler Ebene entwickelten Standards Rechnung tragen. TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten verhältnismäßige Verfahren für die Überprüfung der Domänennamen-Registrierungsdaten verabschieden und umsetzen. Bei diesen Verfahren sollten die in dem Wirtschaftszweig angewandten bewährten Verfahren und, soweit möglich, die Fortschritte im Bereich der elektronischen Identifizierung berücksichtigt werden. Beispiele für Überprüfungsverfahren können Ex-ante-Kontrollen zum Zeitpunkt der Registrierung und Ex-post-Kontrollen nach der Registrierung sein. TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten insbesondere mindestens eine Kontaktmöglichkeit des Domäneninhabers überprüfen.

(112) TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten Domänennamen-Registrierungsdaten, die nicht in den Anwendungsbereich des Datenschutzrechts der Union fallen, z. B. Daten, die juristische Personen betreffen, gemäß der Präambel der Verordnung (EU) 2016/679 öffentlich zugänglich machen müssen. Bei juristischen Personen sollten die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, zumindest den Namen des Domäneninhabers und die Kontakt-Telefonnummer öffentlich zugänglich machen. Die Kontakt-E-Mail-Adresse sollte ebenfalls veröffentlicht werden, sofern sie keine personenbezogenen Daten enthält u. a. durch den Einsatz eines E-Mail-Alias oder eines Funktionskontos. TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen im Einklang mit dem Datenschutzrecht der Unionerhalten. Die Mitgliedstaaten sollten TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, verpflichten, Anträge auf Offenlegung von Domänennamen-Registrierungsdaten von berechtigten Zugangsnachfragern unverzüglich zu beantworten. TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von

Anträgen berechtigter Zugangsnachfrager. Diese Strategien und Verfahren sollten so weit wie möglich etwaigen Leitlinien und den von den Multi-Stakeholder-Governance-Strukturen auf internationaler Ebene entwickelten Standards Rechnung tragen. Das Zugangsverfahren könnte auch die Verwendung einer Schnittstelle, eines Portals oder eines anderen technischen Instruments umfassen, um ein effizientes System für die Anforderung von und den Zugriff auf Registrierungsdaten bereitzustellen. Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses Leitlinien zu solchen Verfahren bereitstellen, bei denen so weit wie möglich den von den Multi-Stakeholder-Governance-Strukturen auf internationaler Ebene entwickelten Standards Rechnung getragen wird. Die Mitgliedstaaten sollten dafür sorgen, dass alle Arten des Zugangs zu personenbezogene und nicht personenbezogenen Domänennamen-Registrierungsdaten kostenfrei sind.

(113) Einrichtungen, die unter diese Richtlinie fallen, sollten der Zuständigkeit des Mitgliedstaats unterliegen, in dem sie niedergelassen sind. Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste sollten jedoch als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie ihre Dienste erbringen; 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, Anbieter von Online-Suchmaschinen oder Anbieter von Plattformen für Dienste sozialer Netzwerke sollten als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie ihre Hauptniederlassung in der Union haben. Einrichtungen der öffentlichen Verwaltung sollten als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie niedergelassen sind. Erbringt die Einrichtung Dienste in mehreren Mitgliedstaaten oder hat sie Niederlassungen in mehreren Mitgliedstaaten, so sollte sie unter die getrennte und parallele Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen. Wenn die Mitgliedstaaten ihre Zuständigkeit ausüben, sollten sie gemäß dem Grundsatz „ne bis in idem“ keine Durchsetzungsmaßnahmen oder Sanktionen mehr als einmal für ein und dasselbe Verhalten verhängen.

(114) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Anbietern von verwalteten Diensten, Anbietern von verwalteten Sicherheitsdiensten, Anbietern von Online-Marktplätzen, Anbietern von Online-Suchmaschinen sowie Anbieter von Plattformen für Dienste sozialer Netzwerke grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. Die Zuständigkeit sollte bei dem Mitgliedstaat liegen, in dem die betreffende Einrichtung ihre Hauptniederlassung in der Union hat. Das Kriterium der Niederlassung im Sinne dieser Richtlinie setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei unerheblich. Dieses Kriterium sollte nicht davon abhängen, ob die Netz- und Informationssysteme an einem bestimmten Ort physisch untergebracht sind; die Existenz und die Nutzung derartiger Systeme stellen an sich keine derartige Hauptniederlassung dar und sind daher kein ausschlaggebendes Kriterium für die Bestimmung der Hauptniederlassung. Die Hauptniederlassung sollte als in dem Mitgliedstaat angesehen sein, an dem in der Union über Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend entschieden wird. In der Regel entspricht dies dem Ort, an dem sich die Hauptverwaltung der Einrichtungen in der Union befindet. 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. Werden solche Entscheidungen nicht in der Union getroffen, ist davon auszugehen, dass sich die Hauptniederlassung in dem Mitgliedstaat befindet, in dem die Einrichtung über eine Niederlassung mit der unionsweit höchsten Beschäftigtenzahl verfügt. Werden die Dienste von einer Unternehmensgruppe ausgeführt, so sollte die Hauptniederlassung des herrschenden Unternehmens als Hauptniederlassung der Unternehmensgruppe gelten.

(115) Wenn ein Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste einen öffentlich zugänglichen rekursiven DNS-Dienst nur als Teil des Internetzugangsdienstes anbietet, so sollte davon ausgegangen werden, dass die Einrichtung der Zuständigkeit aller Mitgliedstaaten unterliegt, in denen sie ihre Dienste erbringt.

(116) Bietet ein DNS-Diensteanbieter, ein TLD-Namenregister, eine Einrichtung, die Domänennamen-Registrierungsdienste erbringt, ein Anbieter von Cloud-Computing-Diensten, ein Anbieter von Rechenzentren, ein Anbieter von Inhaltezustellnetzen, ein verwalteter Diensteanbieter, ein verwalteter Anbieter von Sicherheitsdiensten oder ein Anbieter eines Online-Marktplatzes, einer Online-Suchmaschine oder einer Plattform sozialer Netzwerke, der nicht in der Union niedergelassen ist, Dienste innerhalb der Union an, so sollte er einen Vertreter in der Union benennen. Um festzustellen, ob eine solche Einrichtung in der Union Dienste anbietet, sollte geprüft werden, ob sie beabsichtigt, Personen in einem oder mehreren Mitgliedstaaten Dienste anzubieten. Die bloße Zugänglichkeit der Website einer Einrichtung oder eines Vermittlers von der Union aus oder einer E-Mail-Adresse oder anderer Kontaktdaten sollten zur Feststellung einer solchen Absicht ebenso wenig als ausreichend betrachtet werden wie die Verwendung einer Sprache, die in dem Drittland, in dem die Einrichtung niedergelassen ist, allgemein gebräuchlich ist. Jedoch können andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Dienste in dieser Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern in der Union darauf hindeuten, dass die Einrichtung beabsichtigt, in der Union Dienste anzubieten. Der Vertreter sollte im Auftrag der Einrichtung handeln, und es sollte für die zuständigen Behörden oder CSIRTs möglich sein, sich an ihn zu wenden. Der Vertreter sollte von der Einrichtung ausdrücklich schriftlich beauftragt werden, im Rahmen der sich aus dieser Richtlinie ergebenden Pflichten der Einrichtung in deren Auftrag zu handeln, was auch die Meldung von Sicherheitsvorfällen einschließt.

(117) Um einen klaren Überblick über DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamenregistrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentren, Anbietern von Inhaltszustellnetzen, verwalteten Diensteanbietern, Anbietern von verwalteten Sicherheitsdiensten sowie Anbietern von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für soziale Netzwerke zu gewährleisten, die unionsweit Dienste erbringen, die in den Anwendungsbereich dieser Richtlinie fallen, sollte die ENISA auf der Grundlage der Informationen, die die Mitgliedstaaten gegebenenfalls über für die Selbstregistrierung von Einrichtungen eingerichtete nationale Mechanismen erhalten, ein Register solcher Einrichtungen einrichten und führen. Die zentralen Anlaufstellen sollten der ENISA die Informationen und alle diesbezüglichen Änderungen übermitteln. Um die Richtigkeit und Vollständigkeit der in dieses Register aufzunehmenden Informationen sicherzustellen, können die Mitgliedstaaten der ENISA die in nationalen Registern verfügbaren Informationen über diese Einrichtungen übermitteln. Die ENISA und die Mitgliedstaaten sollten Maßnahmen ergreifen, um die Interoperabilität solcher Register zu fördern und gleichzeitig den Schutz vertraulicher oder als Verschlusssachen eingestufter Informationen zu gewährleisten. Die ENISA sollte geeignete Informationsklassifizierungs- und -verwaltungsprotokolle erstellen, um die Sicherheit und Vertraulichkeit offengelegter Informationen sicherzustellen und den Zugang, die Speicherung und die Übermittlung derartiger Informationen an die vorgesehenen Nutzer zu beschränken.

(118) Werden Informationen, die gemäß Unionsrecht oder nationalem Recht als vertraulich eingestuft sind, im Rahmen dieser Richtlinie ausgetauscht, gemeldet oder auf andere Weise weitergegeben, so sollten die entsprechenden Vorschriften für den Umgang mit Verschlusssachen angewandt werden. Darüber hinaus sollte die ENISA über die Infrastruktur, Verfahren und Vorschriften verfügen, um sensible und als Verschlusssache eingestufte Informationen gemäß den geltenden Sicherheitsvorschriften zum Schutz von EU-Verschlusssachen zu behandeln.

(119) Da Cyberbedrohungen komplexer und technisch ausgereifter werden, hängen eine gute Erkennung dieser Bedrohungen und entsprechende Präventionsmaßnahmen in hohem Maße von einem regelmäßigen Informationsaustausch zwischen den Einrichtungen über Bedrohungen und Schwachstellen ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen, wodurch Einrichtungen Bedrohungen abwehren können, bevor diese in Sicherheitsvorfälle münden, und in der Lage sind, die Auswirkungen von Sicherheitsvorfällen besser einzudämmen und effizienter zu reagieren. In Ermangelung von Leitlinien auf Unionsebene scheinen unterschiedliche Faktoren einen solchen Wissensaustausch verhindert zu haben, insbesondere die nicht geklärte Vereinbarkeit mit den Wettbewerbs- und Haftungsvorschriften.

(120) Die Einrichtungen sollten ermutigt und von den Mitgliedstaaten dabei unterstützt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Sicherheitsvorfälle angemessen zu verhindern, zu erkennen, auf sie zu reagieren, sie zu bewältigen oder in ihrer Wirkung zu begrenzen. Daher muss dafür gesorgt werden, dass auf Unionsebene Vereinbarungen über den freiwilligen Informationsaustausch getroffen werden können. Zu diesem Zweck sollten die Mitgliedstaaten Einrichtungen, wie jene, die Cybersicherheitsdienste und -forschung anbieten, sowie einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Vereinbarungen zum Austausch von Informationen über Cybersicherheit zu beteiligen. Diese Vereinbarungen sollten in Einklang mit den Wettbewerbsvorschriften der Union und dem Datenschutzrecht der Union getroffen werden.

(121) Die Verarbeitung personenbezogener Daten durch wesentliche und wichtige Einrichtungen in dem zur Gewährleistung der Sicherheit von Netz- und Informationssystemen erforderlichen und verhältnismäßigen Umfang könnte auf der Grundlage als rechtmäßig angesehen werden, dass diese Verarbeitung einer rechtlichen Verpflichtung entspricht, der der Verantwortliche gemäß Artikel 6 Absatz 1 Buchstabe c und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 unterliegt. Die Verarbeitung personenbezogener Daten könnte auch für berechtigte Interessen erforderlich sein, die von wesentlichen und wichtigen Einrichtungen sowie von Anbietern von Sicherheitstechnologien und -diensten, die im Namen dieser Einrichtungen handeln, gemäß Artikel 6 Absatz 1 Buchstabe f der Verordnung (EU) 2016/679 wahrgenommen werden, auch wenn eine solche Verarbeitung für Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder die freiwillige Mitteilung relevanter Informationen gemäß dieser Richtlinie erforderlich ist. Maßnahmen im Hinblick auf die Verhütung, Erkennung, Identifizierung, Eindämmung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und der koordinierten Offenlegung von Schwachstellen, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Kompromittierungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools könnten erfordern die Verarbeitung bestimmter Kategorien personenbezogener Daten wie IP-Adressen, URL-Adressen (Uniform Resource Locators – URLs), Domänennamen, E-Mail-Adressen oder, sofern diese personenbezogene Daten anzeigen, Zeitstempel. Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden, zentralen Anlaufstellen und CSIRTs könnte eine rechtliche Verpflichtung darstellen oder als für die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich angesehen werden, die dem jeweiligen Verantwortlichen gemäß Artikel 6 Absatz 1 Buchstabe c oder e und Artikel 6 Absatz 3 der Verordnung (EU) 2016/679 übertragen wurde, oder zur Verfolgung eines berechtigten Interesses der wesentlichen und wichtigen Einrichtungen gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung. Darüber hinaus könnten im nationalen Recht Vorschriften festgelegt werden, die es den zuständigen Behörden, zentralen Anlaufstellen und CSIRTs ermöglichen, besondere Kategorien personenbezogener Daten gemäß Artikel 9 der Verordnung (EU) 2016/679 zu verarbeiten, soweit dies zur Gewährleistung der Sicherheit der Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen erforderlich und verhältnismäßig ist, insbesondere indem geeignete und besondere Maßnahmen zum Schutz der Grundrechte und Interessen natürlicher Personen vorgesehen werden, einschließlich technischer Beschränkungen für die Weiterverwendung solcher Daten und die Anwendung modernster Sicherheits- und Datenschutzvorkehrungen wie Pseudonymisierung oder Verschlüsselung, wenn die Anonymisierung den verfolgten Zweck erheblich beeinträchtigen könnte.

(122) Zur Stärkung der Aufsichtsbefugnisse und der Maßnahmen, die zu einer wirksamen Befolgung der Vorschriften beitragen, sollte diese Richtlinie einen Mindestumfang an Aufsichtsmaßnahmen und -mitteln vorsehen, mit welchen die zuständigen Behörden wesentliche und wichtige Einrichtungen beaufsichtigen können. Darüber hinaus sollte in dieser Richtlinie eine Abgrenzung zwischen den Aufsichtssystemen für wesentliche und für wichtige Einrichtungen vorgenommen werden, um die Verpflichtungen für diese Einrichtungen und für die zuständigen Behörden ausgewogen zu gestalten. Daher sollten wesentliche Einrichtungen einem umfassenden Ex-ante- und Ex-post-Aufsichtssystem unterliegen, während wichtige Einrichtungen einem einfachen, ausschließlich nachträglichen Aufsichtssystem unterliegen sollten. Wichtige Einrichtungen müssten daher die Erfüllung der Anforderungen hinsichtlich der Maßnahmen des Cybersicherheitsrisikomanagements nicht systematisch dokumentieren, während die zuständigen Behörden ein reaktives Ex-post-Aufsichtskonzept anwenden und deshalb nicht generell verpflichtet sein sollten, diese Einrichtungen zu beaufsichtigen. Bei wichtigen Einrichtungen kann eine Ex-post-Aufsicht dadurch ausgelöst werden, dass den zuständigen Behörden Belege oder Hinweise oder Informationen zur Kenntnis gebracht werden, die von ihnen als Anzeichen für eine mögliche Verstöße gegen diese Richtlinie gedeutet werden. Solche Belege, Hinweise oder Informationen könnten beispielsweise den zuständigen Behörden von anderen Behörden, Einrichtungen, Bürgern oder Medien zur Verfügung gestellt werden oder aus anderen Quellen oder öffentlich zugänglichen Informationen herrühren oder sich aus anderen Tätigkeiten der zuständigen Behörden bei der Wahrnehmung ihrer Aufgaben ergeben.

(123) Die Wahrnehmung von Aufsichtsaufgaben durch die zuständigen Behörden sollte die Geschäftstätigkeit der betreffenden Einrichtung nicht unnötig behindern. Wenn die zuständigen Behörden ihre Aufsichtsaufgaben in Bezug auf wesentliche Einrichtungen wahrnehmen, einschließlich der Durchführung von Vor-Ort-Prüfungen und der externen Aufsicht, der Untersuchung von Verstößen gegen diese Richtlinie, der Durchführung von Sicherheitsaudits oder Sicherheitsscans, sollten sie die Auswirkungen auf die Geschäftstätigkeit der betreffenden Einrichtung so gering wie möglich halten.

(124) Im Zusammenhang mit der Ex-ante-Aufsicht sollten die zuständigen Behörden die Möglichkeit haben, darüber zu entscheiden, ob die ihnen zur Verfügung stehenden Aufsichtsmaßnahmen und -mittel unter Wahrung der Verhältnismäßigkeit mit Vorrang angewandt werden. Dies bedeutet, dass die zuständigen Behörden über eine solche Priorisierung auf der Grundlage von Aufsichtsmethoden entscheiden können, die auf einem risikobasierten Ansatz beruhen sollten. Konkret könnten solche Methoden Kriterien oder Benchmarks für die Einstufung wesentlicher Einrichtungen in Risikokategorien und entsprechende Aufsichtsmaßnahmen und -mittel, die für jede

Risikokategorie empfohlen werden, umfassen, wie etwa die Durchführung, Häufigkeit oder Arten der Vor-Ort-Kontrollen, gezielten Sicherheitsprüfungen oder Sicherheitsscans, die Art der verlangten Informationen und der Detaillierungsgrad dieser Informationen. Solche Aufsichtsmethoden könnten auch mit Arbeitsprogrammen einhergehen und regelmäßig bewertet und überprüft werden, auch in Bezug auf Aspekte wie Mittelzuweisung und -bedarf. Bei Einrichtungen der öffentlichen Verwaltung sollten die Aufsichtsbefugnisse im Einklang mit dem jeweiligen nationalen rechtlichen und institutionellen Rahmen ausgeübt werden.

(125) Die zuständigen Behörden sollten sicherstellen, dass ihre Aufsichtsaufgaben in Bezug auf wesentliche und wichtige Einrichtungen von geschulten Fachkräften wahrgenommen werden, die über die für die Wahrnehmung dieser Aufgaben erforderlichen Kompetenzen verfügen sollten, insbesondere im Hinblick auf die Durchführung von Vor-Ort-Prüfungen und die externe Aufsicht, einschließlich der Ermittlung von Schwachstellen in Datenbanken, Hardware, Firewalls, Verschlüsselung und Netzwerken. Diese Inspektionen und die Überwachung sollten objektiv durchgeführt werden.

(126) In hinreichend begründeten Fällen, in denen ihr eine erhebliche Cyberbedrohung oder ein unmittelbar bevorstehendes Risiko bekannt ist, sollte die zuständige Behörde in der Lage sein, unverzüglich Durchsetzungsentscheidungen zu treffen, um einen Sicherheitsvorfall zu verhindern oder darauf zu reagieren.

(127) Für eine wirksame Durchsetzung sollte eine Mindestliste von Durchsetzungsbefugnissen, die bei Verstößen gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Berichtspflichten gemäß dieser Richtlinie ausgeübt werden können, festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Durchsetzung geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes gegen diese Richtlinie, dem entstandenen materiellen oder immateriellen Schaden, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung des entstandenen materiellen oder immateriellen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der Aufsichtsbehörde sowie jedem anderen erschwerenden oder mildernden Umstand. Die Durchsetzungsmaßnahmen, einschließlich Geldbußen, sollten verhältnismäßig sein, und für die Verhängung sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union (die „Charta“), einschließlich des Rechts auf einen wirksamen Rechtsbehelf und ein faires Verfahren sowie der Unschuldsvermutung und des Rechts der Verteidigung, entsprechen.

(128) Mit dieser Richtlinie werden die Mitgliedstaaten nicht verpflichtet, eine strafrechtliche oder zivilrechtliche Haftung gegenüber natürlichen Personen vorzusehen, die dafür verantwortlich sind, dass eine Einrichtung die Bestimmungen dieser Richtlinie für Schäden einhält, die Dritten infolge eines Verstoßes gegen diese Richtlinie entstanden sind.

(129) Um die wirksame Durchsetzung der in dieser Richtlinie festgelegten Verpflichtungen zu gewährleisten, sollte jede zuständige Behörde befugt sein, Geldbußen aufzuerlegen oder ihre Auferlegung zu beantragen.

(130) Wird einer wesentlichen oder wichtigen Einrichtung, bei der es sich um ein Unternehmen handelt, eine Geldbuße auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Wird einer Person, bei der es sich nicht um ein Unternehmen handelt, eine Geldbuße auferlegt, so sollte die zuständige Behörde bei der geeigneten Bemessung der Geldbuße dem allgemeinen Einkommensniveau in dem betreffenden Mitgliedstaat und der wirtschaftlichen Lage der Personen Rechnung tragen. Die Mitgliedstaaten sollten bestimmen können, ob und inwieweit gegen Behörden Geldbußen verhängt werden können. Auch wenn die zuständigen Behörden bereits Geldbußen auferlegt haben, können sie ihre anderen Befugnisse ausüben oder andere Sanktionen verhängen, die in den nationalen Vorschriften zur Umsetzung dieser Richtlinie festgelegt sind.

(131) Die Mitgliedstaaten sollten die strafrechtlichen Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen können. Die Verhängung von strafrechtlichen Sanktionen für Verstöße gegen solche nationalen Vorschriften und von entsprechenden verwaltungsrechtlichen Sanktionen sollte jedoch nicht zu einer Verletzung des Grundsatzes „ne bis in idem“, wie er vom Gerichtshof der Europäischen Union ausgelegt worden ist, führen.

(132) Soweit diese Richtlinie verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei einem schweren Verstoß gegen diese Richtlinie — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende Sanktionen vorsieht. Die Art dieser Sanktionen und die Frage, ob es strafrechtliche oder verwaltungsrechtliche Sanktionen sind, sollte im nationalen Recht geregelt werden.

(133) Um die Wirksamkeit und Abschreckungskraft der Durchsetzungsmaßnahmen bei Verstößen gegen diese Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten relevanten Dienste vorübergehend auszusetzen oder dies zu beantragen, und zu verlangen, dass natürlichen Personen die Ausübung von Leitungsaufgaben auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters vorübergehend untersagt wird. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf die Nutzer sollten solche vorübergehenden Aussetzungen oder Verbote lediglich im Verhältnis zur Schwere des Verstoßes und unter Berücksichtigung der besonderen Umstände des Einzelfalls verhängt werden; hierzu zählen auch die Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, sowie die zur Verhinderung oder Minderung des materiellen oder immateriellen erlittenen Schadens ergriffenen Maßnahmen. Solche vorübergehenden Aussetzungen oder Verbote sollten nur als letztes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betreffende Einrichtung die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich solche vorübergehenden Aussetzungen oder Verbote beziehen, erfüllen. Für die Anwendung solcher vorübergehenden Aussetzungen oder Verbote sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und der Verteidigungsrechte, entsprechen.

(134) Um sicherzustellen, dass die Einrichtungen ihren Verpflichtungen aus dieser Richtlinie nachkommen, sollten die Mitgliedstaaten bei Aufsichts- und Durchsetzungsmaßnahmen zusammenarbeiten und einander dabei unterstützen, insbesondere wenn eine Einrichtung Dienste in mehr als einem Mitgliedstaat erbringt oder ihre Netz- und Informationssysteme in einem anderen Mitgliedstaat als demjenigen angesiedelt sind, in dem sie Dienste erbringt. Bei der Bereitstellung von Unterstützung sollte die ersuchte zuständige Behörde im Einklang mit den nationalen Rechtsvorschriften Aufsichts- oder Durchsetzungsmaßnahmen ergreifen. Um das reibungslose Funktionieren der Amtshilfe im Rahmen dieser Richtlinie sicherzustellen, sollten die zuständigen Behörden die Kooperationsgruppe als Forum nutzen, um Fälle und einzelne Amtshilfeersuchen zu erörtern.

(135) Um eine wirksame Aufsicht und Durchsetzung insbesondere in einem Fall mit grenzüberschreitender Dimension zu gewährleisten, sollte ein Mitgliedstaat, bei dem ein Amtshilfeersuchen eingegangen ist, in einem dem Ersuchen entsprechenden Umfang geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die Einrichtung, die Gegenstand des Ersuchens ist und die im Hoheitsgebiet jenes Mitgliedstaates Dienste anbietet oder ein Netz- und Informationssystem betreibt, ergreifen.

(136) Mit dieser Richtlinie sollten Regeln für die Zusammenarbeit zwischen den zuständigen Behörden und den Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 festgelegt werden, um gegen Verstöße gegen diese Richtlinie im Zusammenhang mit personenbezogenen Daten vorzugehen.

(137) Die Richtlinie sollte darauf abzielen, auf Ebene der wesentlichen und wichtigen Einrichtungen ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Berichtspflichten im Bereich der Cybersicherheit sicherzustellen. Daher sollten die Leitungsorgane der wesentlichen und wichtigen Einrichtungen die Risikomanagementmaßnahmen im Bereich der Cybersicherheit genehmigen und deren Umsetzung überwachen.

(138) Um auf der Grundlage dieser Richtlinie ein hohes gemeinsames Cybersicherheitsniveau in der Union zu gewährleisten, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Richtlinie zu erlassen, in denen festgelegt wird, welche Kategorien wesentlicher und wichtiger Einrichtungen zur Verwendung bestimmter zertifizierter IKT-Produkte, -Dienste und -Prozesse oder zur Erlangung eines Zertifikats im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung verpflichtet sind. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung [22] niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

[22] ABl. L 123 vom 12.5.2016, S. 1.

(139) Um einheitliche Bedingungen für die Durchführung dieser Richtlinie zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden, um die für die Arbeitsweise der Kooperationsgruppe erforderlichen Verfahrensregelungen und die technischen und methodischen sowie sektorspezifischen Anforderungen an die Risikomanagementmaßnahmen im Bereich der Cybersicherheit festzulegen und die Art der Informationen, das Format und das Verfahren von Sicherheitsvorfällen, Cyberbedrohungen und Meldungen über Beinahe-Vorfälle und erhebliche Cyberbedrohungen sowie Fälle, in denen ein Sicherheitsvorfall als erheblich anzusehen ist, näher zu bestimmen. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([23]) ausgeübt werden.

(140) Die Kommission sollte diese Richtlinie regelmäßig nach Abstimmung mit den Interessenträgern überprüfen, insbesondere um festzustellen, ob angesichts veränderter gesellschaftlicher, politischer oder technischer Bedingungen oder veränderter Marktbedingungen Änderungen vorgeschlagen werden sollten. Im Rahmen dieser Überprüfungen sollte die Kommission die Bedeutung der Größe der betreffenden Einrichtungen und der in den Anhängen dieser Richtlinie genannten Sektoren, Teilsektoren und Arten von Einrichtungen für das Funktionieren von Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewerten. Die Kommission sollte unter anderem prüfen, ob Anbieter die in den Anwendungsbereich dieser Richtlinie fallen und die als sehr große Online-Plattformen im Sinne des Artikels 33 der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates ([24]) benannt sind, als wesentliche Einrichtungen im Sinne dieser Richtlinie ermittelt werden könnten.

(141) Mit dieser Richtlinie werden neue Aufgaben für die ENISA geschaffen, wodurch ihre Rolle gestärkt wird, und sie könnte auch dazu führen, dass die ENISA ihre bestehenden Aufgaben gemäß der Verordnung (EU) 2019/881 auf einer höheren Ebene als zuvor ausführen muss. Um sicherzustellen, dass die ENISA über die erforderlichen finanziellen und personellen Ressourcen verfügt, um bestehende und neue Aufgaben im Rahmen ihrer Aufgaben zu erledigen und um etwaigen höheren Anforderungen, die sich aus ihrer erweiterten Rolle ergeben, gerecht zu werden, sollte ihr Haushalt entsprechend aufgestockt werden. Um eine effiziente Nutzung der Ressourcen zu gewährleisten, sollte die ENISA außerdem eine größere Flexibilität bei der Art und Weise erhalten, in der es ihr möglich ist, die Ressourcen intern zuzuweisen, damit sie ihre Aufgaben wirksam wahrnehmen und die Erwartungen erfüllen kann.

(142) Da das Ziel dieser Richtlinie, nämlich die Erreichung eines hohen gemeinsamen Cybersicherheitsniveaus in der gesamten Union, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen ist, kann die Union in Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Richtlinie nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(143) Diese Richtlinie steht im Einklang mit den Grundrechten und den mit der Charta anerkannten Grundsätzen, insbesondere dem Recht auf Achtung des Privatlebens und der privaten Kommunikation, dem Recht auf Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Recht auf Eigentum, dem Recht auf einen wirksamen Rechtsbehelf und ein faires Gerichtsverfahren, der Unschuldsvermutung und der Verteidigungsrechte. Das Recht auf einen wirksamen Rechtsbehelf erstreckt sich auf die Empfänger von Diensten, die von wesentlichen und wichtigen Einrichtungen erbracht werden. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden.

(144) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([25]) angehört und hat am 11. März 2021 eine Stellungnahme ([26]) abgegeben —

([23]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

([24]) Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. L 277 vom 27.10.2022, S. 1).

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

([26]) ABl. C 183 vom 11.5.2021, S. 3.

HABEN FOLGENDE RICHTLINIE ERLASSEN:

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.

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.

(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 ([27]) und 2013/40/EU ([28]) des Europäischen Parlaments und des Rates sowie der Richtlinie (EU) 2022/2557.

(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.

([27]) 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).

([28]) 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).

(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.

(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.

(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

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;

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 ([29]);

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

([29]) 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).

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;

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 ([30]);

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 ([31]);

29. „Online-Suchmaschine“ eine Online-Suchmaschine im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates ([32]);

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;

([30]) 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).

([31]) 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).

([32]) 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).

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;

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;

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;

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.

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.

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.

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;

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

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.

(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.

(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;

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.

(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;

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.

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.

(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.

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.

(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.

(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;

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.

(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) 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.

(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.

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:

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 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:

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

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) 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.

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,

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.

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;

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:

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) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wesentliche 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;

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.

(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.

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.

(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.

(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.

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.

Geschehen zu Straßburg am 14. Dezember 2022.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*
R. METSOLA	M. BEK

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
		— 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

Sektor	Teilsektor	Art der Einrichtung
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
		— 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])

Sektor	Teilsektor	Art der Einrichtung
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
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

Sektor	Teilsektor	Art der Einrichtung
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
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).

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
	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

Sektor	Teilsektor	Art der Einrichtung
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).

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
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

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
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
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

Richtlinie (EU) 2016/1148	Vorliegende Richtlinie
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

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. April 2019

über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

(Text von Bedeutung für den EWR)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme sowie elektronische Kommunikationsnetze und -dienste spielen eine lebenswichtige Rolle in der Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnologien (IKT) bilden das Rückgrat der komplexen Systeme, die alltägliche gesellschaftliche Tätigkeiten unterstützen und unsere Volkswirtschaften in Schlüsselsektoren wie Gesundheit, Energie, Finanzen und Verkehr aufrechterhalten und die insbesondere dafür sorgen, dass der Binnenmarkt reibungslos funktioniert.

(2) Die Nutzung von Netz- und Informationssystemen durch Bürger, Organisationen und Unternehmen ist mittlerweile in der Union allgegenwärtig. Digitalisierung und Konnektivität entwickeln sich zu Kernmerkmalen einer ständig steigenden Zahl von Produkten und Dienstleistungen; mit dem Aufkommen des Internets der Dinge dürften in den nächsten Jahrzehnten eine extrem hohe Zahl vernetzte digitale Geräte unionsweit Verbreitung finden. Zwar sind immer mehr Geräte mit dem Internet vernetzt, doch verfügen sie über eine nur unzureichende Cybersicherheit, da die Sicherheit und Abwehrfähigkeit dieser Geräte schon bei der Konzeption nicht ausreichend berücksichtigt wurden. In diesem Zusammenhang führt das geringe Maß an Zertifizierung dazu, dass Personen, Organisationen und Unternehmen die IKT-Produkte, -Dienste und -prozesse nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert werden, wodurch das Vertrauen in digitale Lösungen untergraben wird. Netz- und Informationssysteme können uns das Leben in jeder Hinsicht erleichtern und das Wirtschaftswachstum der Union anzukurbeln. Sie spielen eine tragende Rolle bei der Verwirklichung des digitalen Binnenmarkts.

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personen wie Kinder ausgesetzt sind. Um diesen Gefahren zu begegnen, gilt es, alle für die Erhöhung der Cybersicherheit in der Union notwendigen Maßnahmen zu ergreifen, damit die Netz- und Informationssysteme, die Kommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Bürgern, Organisationen und Unternehmen — von kleinen und mittleren Unternehmen (KMU) im Sinne der Empfehlung 2003/361/EG der Kommission ([4]) bis zu Betreibern kritischer Infrastrukturen — genutzt werden, besser vor Cyberbedrohungen geschützt sind.

([1]) ABl. C 227 vom 28.6.2018, S. 86.
([2]) ABl. C 176 vom 23.5.2018, S. 29.
([3]) Stellungnahme des Europäischen Parlaments vom 12. März 2019 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 9. April 2019.
([4]) Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36).

(4) Durch das Zurverfügungstellung einschlägiger Informationen für die Öffentlichkeit trägt die mit der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates ([5]) errichtete Agentur der Europäischen Union für Netz- und Informationssicherheit (im Folgenden „ENISA") zur Entwicklung der Cybersicherheitsbranche in der Union, insbesondere von KMU und Start-ups, bei. Die ENISA sollte sich um eine engere Zusammenarbeit mit Universitäten und Forschungseinrichtungen bemühen, um einen Beitrag zur Verringerung der Abhängigkeit von Cybersicherheitsprodukten und -diensten von außerhalb der Union zu leisten und die Lieferketten innerhalb der Union zu stärken.

(5) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren Schutz. Obwohl jedoch die Cyberangriffe häufig grenzüberschreitend sind, sind die Zuständigkeiten und Reaktionen der für die Cybersicherheit und für die Strafverfolgung zuständigen Behörden vor allem national. Sicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten Union empfindlich stören. Notwendig sind daher effektive und koordinierte Maßnahmen sowie ein Krisenmanagement auf Unionsebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für europäische Solidarität und gegenseitige Hilfe. Zudem sind daher eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und der Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen, Herausforderungen und Bedrohungen — auf Unionsebene und auf globaler Ebene — für die Entscheidungsträger, die Branche und die Nutzer gleichermaßen wichtig.

(6) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbauen und sich wechselseitig verstärkende Ziele unterstützen würde. Diese Ziele beinhalten eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit, einen besseren Informationsaustausch und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die Maßnahmen der Mitgliedstaaten vor allem dann ergänzen könnten, wenn es zu grenzüberschreitenden Sicherheitsvorfällen und -krisen von großem Ausmaß kommt, unter Berücksichtigung der Bedeutung der Bewahrung und Verbesserung der nationalen Fähigkeiten zur Reaktion auf Cyberbedrohungen jeglichen Umfangs.

(7) Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürger, Organisationen und Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Da Sicherheitsvorfälle das Vertrauen in Anbieter digitaler Dienste und in den digitalen Binnenmarkt als solchen insbesondere unter den Verbrauchern untergraben, sollte dieses Vertrauen dadurch gestärkt werden, dass auf transparente Art und Weise Informationen über das Niveau der Sicherheit von IKT-Produkten, -Diensten und -Prozessen bereitgestellt werden, wobei betont wird, dass auch eine Cybersicherheitszertifizierung auf hohem Niveau nicht garantieren kann, dass ein IKT-Produkt, -Dienst oder -Prozess völlig sicher ist. Eine Stärkung des Vertrauens kann durch eine unionsweite Zertifizierung erleichtert werden, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

(8) Cybersicherheit ist nicht nur eine Frage der Technologie, sondern eine, bei der das menschliche Verhalten ebenso wichtig ist. Daher sollte die „Cyberhygiene", also einfache Routinemaßnahmen, durch die, wenn sie von Bürgern, Organisationen und Unternehmen regelmäßig umgesetzt und durchgeführt werden, die Risiken von Cyberbedrohungen so gering wie möglich gehalten werden, nachdrücklich gefördert werden.

(9) Um die Cybersicherheitsstrukturen der Union zu stärken, müssen die Fähigkeiten der Mitgliedstaaten, umfassend auf Cyberbedrohungen — einschließlich grenzüberschreitender Sicherheitsvorfälle — zu reagieren, erhalten und ausgebaut werden.

(10) Die Unternehmen und die einzelnen Verbraucher sollten über präzise Informationen darüber verfügen, auf welcher Vertrauenswürdigkeitsstufe die Sicherheit ihrer IKT-Produkte, -Dienste und -Prozesse zertifiziert wurde. Allerdings bietet kein IKT-Produkt oder -dienst hundertprozentige Cybersicherheit weshalb grundlegenden Prinzipien der Cyberhygiene verbreitet werden sollten und ihnen Vorrang eingeräumt werden sollte. Angesichts der zunehmenden Verbreitung von Geräten des Internets der Dinge kann die Privatwirtschaft zahlreiche freiwillige Maßnahmen treffen, um das Vertrauen in die Sicherheit von IKT-Produkten, -Diensten und -Prozessen zu stärken.

(11) Moderne IKT-Produkte und -Systeme weisen oft einen oder mehrere von Dritten entwickelte Technologien und Bestandteile wie Software-Module, Bibliotheken oder Programmierschnittstellen auf und sind von diesen abhängig. Diese „Abhängigkeit" könnte zusätzliche Risiken im Bereich der Cybersicherheit bergen, da sich Sicherheitslücken in Bestandteilen Dritter auch auf die Sicherheit von IKT-Produkten, -Diensten, und -Prozessen auswirken könnten. In vielen Fällen ermöglicht die Aufdeckung und Dokumentierung solcher „Abhängigkeiten" den Endnutzern von IKT-Produkten, -Diensten und -Prozessen die Verbesserung ihres Risikomanagements im Bereich der Cybersicherheit, indem beispielsweise die Behandlung von Sicherheitslücken im Bereich der Cybersicherheit durch die Nutzer und deren Abhilfeverfahren verbessert werden.

([5]) Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (ABl. L 165 vom 18.6.2013, S. 41).

(12) Organisationen, Hersteller oder Diensteanbieter, die an der Konzeption und Entwicklung von IKT-Produkten, -Diensten und -Prozessen beteiligt sind, sollten dazu angehalten werden, in den ersten Phasen der Konzeption und Entwicklung Maßnahmen durchzuführen, um die Sicherheit dieser Produkte, Dienste und Prozesse möglichst weitgehend zu schützen, in dem sie davon ausgehen, dass Cyberangriffe vorliegen, und deren Folgen vorwegzunehmen und so gering wie möglich zu halten (konzeptionsintegrierte Sicherheit — security by design). Die Sicherheit sollte während der gesamten Lebensdauer des IKT-Produkts, -Dienstes oder -Prozesses berücksichtigt werden, wobei die Konzeptions- und Entwicklungsprozesse ständig weiterentwickelt werden sollten, um das Risiko von Schäden durch eine böswillige Nutzung zu verringern.

(13) Unternehmen, Organisationen und der öffentliche Sektor sollten die von ihnen konzipierten IKT-Produkte, -Dienste oder -Prozesse so konfigurieren, dass ein höheres Maß an Sicherheit gewährleistet ist, das es dem ersten Nutzer ermöglicht, eine Standardkonfiguration mit den sichersten möglichen Einstellungen („security by default“) zu erhalten; somit wären die Nutzer in geringerem Maße der Belastung ausgesetzt, ein IKT-Produkt, -einen IKT-Dienst oder einen IKT-Prozess angemessen konfigurieren zu müssen. Die Sicherheit durch Voreinstellungen („security by default“) sollte weder eine umfangreiche Konfiguration erfordern, noch spezifische technische Kenntnisse oder ein nicht offensichtliches Verhalten seitens des Nutzers, und sie sollte dort, wo sie implementiert wurde, einfach und zuverlässig funktionieren. Wenn im Einzelfall eine Risiko- und Nutzbarkeitsanalyse zu dem Ergebnis führt, dass eine solche vordefinierte Einstellung nicht machbar ist, sollten die Nutzer aufgefordert werden, die sicherste Einstellung zu wählen.

(14) Mit der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates ([6]) wurde die ENISA als Beitrag zu den Zielen errichtet, innerhalb der Union eine hohe und effektive Netz- und Informationssicherheit zu gewährleisten und eine Kultur der Netz- und Informationssicherheit zu entwickeln, die Bürgern, Verbrauchern, Unternehmen und öffentlicher Verwaltung zugute kommt. Mit der Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates ([7]) wurde das Mandat der ENISA bis März 2012 verlängert. Durch die Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates ([8]) wurde das Mandat der ENISA nochmals bis zum 13. September 2013 verlängert. Mit der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates wurde das Mandat der ENISA bis zum 19. Juni 2020 verlängert.

(15) Die Union hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde die EU-Cybersicherheitsstrategie der Europäischen Union verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dient. Im Zuge ihrer Bemühung, den Online-Schutz der Bürger zu verbessern, hat die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([9]) den ersten Rechtsakt auf dem Gebiet der Cybersicherheit erlassen. Mit der Richtlinie (EU) 2016/1148 wurden Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt und ferner Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind, wie Energie, Verkehr, Trinkwasserlieferung und -versorgung, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, digitale Infrastruktur sowie für Anbieter zentraler digitaler Dienste (Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze) eingeführt.

Eine zentrale Aufgabe bei der Umsetzung dieser Richtlinie wurde dabei der ENISA zugewiesen. Darüber hinaus ist die wirksame Bekämpfung der Cyberkriminalität als ein Aspekt bei der Verfolgung des übergeordneten Ziels einer hohen Cybersicherheit ein wichtiger Schwerpunkt der Europäischen Sicherheitsagenda. Andere Rechtsakte wie die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([10]) und die Richtlinie 2002/58/EG ([11]) sowie die Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([12]) tragen auch zu einem hohen Maß an Cybersicherheit im digitalen Binnenmarkt bei.

([6]) Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1).

([7]) Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 293 vom 31.10.2008, S. 1).

([8]) Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 165 vom 24.6.2011, S. 3).

([9]) Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

([10]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([11]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

([12]) Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) (ABl. L 321 vom 17.12.2018, S. 36).

(16) Seit der Verabschiedung der Cybersicherheitsstrategie der Europäischen Union im Jahr 2013 und der letzten Überarbeitung des Mandats der ENISA hat sich der gesamtpolitische Rahmen deutlich verändert, da das globale Umfeld nun von größeren Unwägbarkeiten und geringerer Sicherheit geprägt ist. Vor diesem Hintergrund und im Kontext der positiven Entwicklung der Rolle der ENISA als ein Bezugspunkt für Beratung und Sachkenntnis und als Vermittlerin in Bezug auf Zusammenarbeit und den Aufbau von Fähigkeiten sowie angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle im veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie die Union wirksam dabei unterstützen kann, auf die Herausforderungen im Bereich der Cybersicherheit zu reagieren, die sich aus der grundlegend veränderten Cyberbedrohungslandschaft ergeben und für die — wie in der Bewertung der ENISA bestätigt — das laufende Mandat nicht ausreicht.

(17) Die mit dieser Verordnung errichtete ENISA sollte Rechtsnachfolgerin der durch die Verordnung (EU) Nr. 526/2013 errichteten ENISA sein. Die ENISA sollte die Aufgaben wahrnehmen, die ihr mit dieser Verordnung und anderen Rechtsakten der Union im Bereich der Cybersicherheit übertragen werden, indem sie unter anderem Beratung bietet und Sachkenntnis bereitstellt indem sie die Rolle eines Informations- und Wissenszentrums der Union übernimmt. Sie sollte den Austausch bewährter Verfahren zwischen den Mitgliedstaaten und privaten Interessenträgern fördern, der Kommission und den Mitgliedstaaten strategische Vorschläge unterbreiten, als Bezugspunkt für sektorspezifische politische Initiativen der Union im Bereich der Cybersicherheit dienen und die operative Zusammenarbeit sowohl zwischen den Mitgliedstaaten als auch zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union fördern.

(18) Mit dem Einvernehmlichen Beschluss 2004/97/EG, Euratom der auf Ebene der Staats- und Regierungschefs vereinigten Vertreter der Mitgliedstaaten ([13]), legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu benennenden Stadt haben soll. Der Sitzmitgliedstaat der ENISA sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der ENISA gewährleisten. Damit die ENISA ihre Aufgaben ordnungsgemäß und effizient erfüllen, Personal einstellen und binden und die Effizienz der Vernetzungsmaßnahmen steigern kann, ist es unbedingt erforderlich, sie an einem geeigneten Standort anzusiedeln, der unter anderem eine angemessene Verkehrsanbindung sowie Einrichtungen für die Ehepartner und Kinder des Personals der ENISA bietet. Die erforderlichen Modalitäten sollten in einem Abkommen zwischen der ENISA und dem Sitzmitgliedstaat festgelegt werden, das nach Billigung durch den Verwaltungsrat der ENISA geschlossen wird.

(19) Angesichts der zunehmenden Bedrohungen und Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die ENISA erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Ökosystem der Organisationen gerecht werden kann, die das digitale Ökosystem der Union verteidigen, sodass die ENISA die ihr mit dieser Verordnung übertragenen Aufgaben wirksam erfüllen kann.

(20) Die ENISA sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und als Bezugspunkt fungieren, wobei sie durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren, die Transparenz ihrer Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, Vertrauen in den Binnenmarkt schafft. Die ENISA sollte die Bemühungen der Mitgliedstaaten aktiv unterstützen und vorausgreifend zu den Bemühungen der Union beitragen und ihre Aufgaben in uneingeschränkter Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union und den Mitgliedstaaten wahrnehmen, wobei Doppelarbeiten vermieden und Synergien gefördert werden sollten. Außerdem sollte sich die ENISA auf die Beiträge des Privatsektors und anderer einschlägiger Interessenträger sowie auf die Zusammenarbeit mit ihnen stützen. Mit einer Reihe von Aufgaben sollte bei gleichzeitiger Wahrung der Flexibilität in ihrer Tätigkeit vorgegeben werden, wie die ENISA ihre Ziele erreichen soll.

(21) Damit sie die operative Zusammenarbeit zwischen den Mitgliedstaaten angemessen unterstützen kann, sollte die ENISA ihre technischen und menschlichen Fähigkeiten und Fertigkeiten weiter ausbauen. Die ENISA sollte ihr Know-how und ihre Fähigkeiten vergrößern. Die ENISA und die Mitgliedstaaten könnten auf freiwilliger Basis Programme für die Entsendung von nationalen Sachverständigen an die ENISA, die Bildung von Pools von Sachverständigen und den Austausch von Personal entwickeln.

(22) Die ENISA sollte die Kommission mit Beratung, Stellungnahmen und Analysen zu allen Angelegenheiten der Union, die mit der Ausarbeitung, Aktualisierung und Überprüfung von Strategien und Rechtsvorschriften im Bereich der Cybersicherheit und den diesbezüglichen sektorenspezifischen Aspekten zusammenhängen, unterstützen, damit die Strategien und Rechtsvorschriften der Union mit einer Cybersicherheitsdimension zweckdienlicher gestaltet werden und die kohärente Umsetzung dieser Strategien und Rechtsvorschriften auf nationaler Ebene ermöglicht wird. Für sektorspezifische Strategien und Rechtsetzungsinitiativen der Union im Zusammenhang mit der Cybersicherheit sollte die ENISA als Bezugspunkt für Beratung und Sachkenntnis dienen. Die ENISA sollte dem Europäischen Parlament regelmäßig über ihre Tätigkeiten Bericht erstatten.

([13]) Einvernehmlicher Beschluss 2004/97/EG, Euratom der auf Ebene der Staats- und Regierungschefs vereinigten Vertreter der Mitgliedstaaten vom 13. Dezember 2003 über die Festlegung der Sitze bestimmter Ämter, Behörden und Agenturen der Europäischen Union (ABl. L 29 vom 3.2.2004, S. 15).

(23) Der öffentliche Kern des offenen Internets, d. h. seine wichtigsten Protokolle und Infrastrukturen, die ein globales öffentliches Gut sind, stellt die wesentlichen Funktionen des Internets als Ganzes bereit und bildet die Grundlage für dessen normalen Betrieb. Die ENISA sollte die Sicherheit und Stabilität dieses öffentlichen Kerns des offenen Internets unterstützen, unter anderem — aber nicht beschränkt auf — die wichtigsten Protokolle (insbesondere DNS, BGP und IPv6), den Betrieb des „Domain Name System" (DNS) (wie den Betrieb aller Domänen der obersten Ebene) und den Betrieb der Root-Zone.

(24) Die ENISA hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der Richtlinie (EU) 2016/1148 und anderer maßgeblicher Rechtsakte zu Aspekten der Cybersicherheit, zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit ist klar, dass die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe durch ein umfassenderes und ressortübergreifendes Konzept unterstützt werden müssen.

(25) Die ENISA sollte die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union in ihrem Bemühen um den Auf- und Ausbau der Fähigkeiten und der Bereitschaft zur Verhütung, Erkennung und Bewältigung von Cyberbedrohungen und von Sicherheitsvorfällen im Zusammenhang mit der Netz- und Informationssicherheit unterstützen. So sollte die ENISA den Auf- und Ausbau der in der Richtlinie (EU) 2016/1148 vorgesehenen Reaktionsteams für Computersicherheitsverletzungen (im Folgenden „CSIRTs") der Mitgliedstaaten und der Union unterstützen, damit sie ein unionsweit hohes Maß an Ausgereiftheit erreichen. Die Tätigkeiten der ENISA im Zusammenhang mit den operativen Kapazitäten der Mitgliedstaaten sollten die Maßnahmen der Mitgliedstaaten zur Erfüllung ihrer Verpflichtungen aus der Richtlinie (EU) 2016/1148 aktiv unterstützen und diese daher nicht ersetzen.

(26) Zudem sollte die ENISA auf Ersuchen die Ausarbeitung und Aktualisierung von Strategien im Bereich der Netz- und Informationssysteme auf Unionsebene und, auf Anfrage, auf Ebene der Mitgliedstaaten, insbesondere der Cybersicherheit, unterstützen und sollte die Verbreitung solcher Strategien fördern und die Fortschritte bei deren Umsetzung verfolgen. Die ENISA sollte auch dazu beitragen, den Bedarf an Ausbildungsmaßnahmen und Ausbildungsmaterial, auch in Bezug auf öffentliche Stellen, zu decken, und gegebenenfalls in großem Umfang auf der Grundlage des Referenzrahmens für digitale Kompetenzen der Bürger Ausbilder weiterbilden, um die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union darin zu unterstützen, eigene Ausbildungskapazitäten aufzubauen.

(27) Die ENISA sollte die Mitgliedstaaten im Bereich der Sensibilisierung und Ausbildung in Bezug auf die Cybersicherheit unterstützen, indem sie eine engere Koordinierung und den Austausch von bewährten Verfahren zwischen den Mitgliedstaaten fördert. Diese Unterstützung könnte darin bestehen, dass sie ein Netz von nationalen Bildungskontaktstellen und eine Ausbildungsplattform zur Cybersicherheit entwickelt. Das Netz der nationalen Bildungskontaktstellen könnte im Rahmen des Netzes der nationalen Verbindungsbeamten betrieben werden und einen Ausgangspunkt für die zukünftige Koordinierung innerhalb der Mitgliedstaaten bilden.

(28) Die ENISA sollte die durch die Richtlinie (EU) 2016/1148 eingesetzte Kooperationsgruppe bei der Wahrnehmung ihrer Aufgaben unterstützen, indem sie vor allem ihre Sachkenntnis und Beratung zur Verfügung stellt und den Austausch bewährter Verfahren erleichtert, unter anderem was die Ermittlung von Betreibern wesentlicher Dienste durch die Mitgliedstaaten in Bezug auf Risiken und Sicherheitsvorfälle anbelangt, auch mit Blick auf grenzüberschreitende Abhängigkeiten.

(29) Die ENISA sollte als Anreiz für die Zusammenarbeit zwischen dem öffentlichen und privaten Sektor, vor allem als Beitrag zum Schutz kritischer Infrastrukturen, den Informationsaustausch in und zwischen Sektoren, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, unterstützen, indem sie bewährte Verfahren und Leitfäden zu den verfügbaren Instrumenten und Verfahren bereitstellt und aufzeigt, wie regulatorische Fragen im Zusammenhang mit der Informationsweitergabe geklärt werden können, wobei dies beispielsweise durch die Erleichterung des Aufbaus sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres) erreicht werden soll.

(30) In Anbetracht der Tatsache, dass die möglichen negativen Auswirkungen von Sicherheitslücken bei IKT-Produkten, -Diensten und -Prozessen stetig zunehmen, spielen die Aufdeckung und die Behebung solcher Sicherheitslücken eine wichtige Rolle bei der Verringerung der Gesamtrisiken im Bereich der Cybersicherheit. Es hat sich gezeigt, dass die Zusammenarbeit zwischen Organisationen, Herstellern oder Anbietern besonders gefährdeter IKT-Produkte, -Dienste oder -Prozesse sowie Mitgliedern der Forschungsgemeinschaft im Bereich der Cybersicherheit und Regierungen, die diese Sicherheitslücken aufspüren, sowohl die Aufdeckung als auch die Behebung von Sicherheitslücken bei IKT-Produkten, -Diensten oder -Prozessen erheblich verbessert. Die koordinierte Offenlegung von Sicherheitslücken erfolgt in einem strukturierten Prozess der Zusammenarbeit, in dem Sicherheitslücken dem Eigentümer des Informationssystems gemeldet werden, wodurch die Organisation Gelegenheit zur Diagnose und Behebung der Sicherheitslücke erhält, bevor detaillierte Informationen über die Sicherheitslücke an Dritte oder die Öffentlichkeit weitergegeben werden. Das Verfahren sieht ferner eine Koordinierung zwischen demjenigen, der die Sicherheitslücke aufgespürt hat, und der Organisation im Hinblick auf die Veröffentlichung jener Sicherheitslücke vor. Grundsätze für die koordinierte Offenlegung von Sicherheitslücken könnten eine wichtige Rolle bei den Bemühungen der Mitgliedstaaten um die Verbesserung der Cybersicherheit spielen.

(31) Die ENISA sollte die freiwillig bereitgestellten nationalen Berichte der CSIRTs und des interinstitutionellen IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union („CERT-EU"), welche mit der zwischen dem Europäischen Parlament, dem Europäischen Rat, dem Rat der Europäischen Union, der Europäischen Kommission, dem Gerichtshof der Europäischen Union, der Europäischen Zentralbank, dem Europäischen Rechnungshof, dem Europäischen Auswärtigen Dienst, dem Europäischen Wirtschafts- und Sozialausschuss, dem Europäischen Ausschuss der Regionen und der Europäischen Investitionsbank geschlossenen Vereinbarung über die Organisation und die Funktionsweise eines IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) ([14]) errichtet wurde, zusammenstellen und auswerten, um einen Beitrag zur Aufstellung gemeinsamer Verfahren für den Informationsaustausch, zur Festlegung der Sprache und zu terminologischen Vereinbarungen zu leisten. In diesem Zusammenhang sollte die ENISA im Rahmen der Richtlinie (EU) 2016/1148, die die Grundlage für den freiwilligen Austausch technischer Informationen auf operativer Ebene innerhalb des Netzwerks von Computer-Notfallteams (im Folgenden „CSIRTs-Netz") gemäß der genannten Richtlinie geschaffen hat, auch den Privatsektor einbeziehen.

(32) Die ENISA sollte dazu beitragen, dass bei massiven grenzüberschreitenden Vorfällen und -krisen in Bezug auf Cybersicherheit eine Reaktion auf Unionsebene erfolgt. Diese Aufgabe sollte ENISA entsprechend ihrem Mandat gemäß dieser Verordnung und einem Ansatz ausführen, der von den Mitgliedstaaten im Zusammenhang mit der Empfehlung (EU) 2017/1584 ([15]) der Kommission und den Schlussfolgerungen des Rates vom 26. Juni 2018 zu einer koordinierten Reaktion auf große Cybersicherheitsvorfälle und -krisen festzulegen ist. Zu dieser Aufgabe könnte auch gehören, dass sie relevante Informationen zusammenstellt und den Kontakt zwischen dem CSIRTs-Netz und den Fachkreisen sowie den für das Krisenmanagement zuständigen Entscheidungsträgern erleichtert. Zudem sollte die ENISA die operative Zusammenarbeit zwischen den Mitgliedstaaten auf Ersuchen eines oder mehrerer Mitgliedstaaten unterstützen, indem sie die Bewältigung der Sicherheitsvorfälle aus technischer Sicht übernimmt, indem sie den Austausch entsprechender technischer Lösungen zwischen den Mitgliedstaaten erleichtert und Beiträge für die Öffentlichkeitsarbeit liefert. Die ENISA sollte die operative Zusammenarbeit unterstützen, indem sie die Modalitäten einer solchen Zusammenarbeit im Rahmen regelmäßig stattfindender Cybersicherheitsübungen testet.

(33) Zur Unterstützung der operativen Zusammenarbeit sollte die ENISA im Wege einer strukturierten Zusammenarbeit auf den bei der CERT-EU vorhandenen technischen und operativen Sachverstand zurückgreifen. Eine solche strukturierte Zusammenarbeit könnte auf der Sachkenntnis der ENISA aufbauen. Für die Festlegung der praktischen Aspekte einer solchen Kooperation und zur Vermeidung von Doppelarbeit sollten gegebenenfalls zwischen den beiden Stellen die hierfür notwendigen Modalitäten festgelegt werden.

(34) Entsprechend ihrer Aufgabe, die operative Zusammenarbeit im Rahmen des CSIRTs-Netzes zu unterstützen, sollte die ENISA in der Lage sein, die Mitgliedstaaten auf deren Ersuchen hin zu unterstützen, indem sie diese beispielsweise berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können, die technische Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen erleichtert oder sicherstellt, dass Cyberbedrohungen und Sicherheitsvorfälle analysiert werden. Die ENISA sollte die technische Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen insbesondere dadurch erleichtern, dass sie den freiwilligen Austausch technischer Lösungen zwischen den Mitgliedstaaten unterstützt oder kombinierte technische Informationen — etwa über technische Lösungen, die von den Mitgliedstaaten freiwillig bereitgestellt werden — erstellt. Der Empfehlung (EU) 2017/1584 zufolge sollten die Mitgliedstaaten in gutem Glauben untereinander sowie mit der ENISA Informationen über massive Vorfälle und -krisen in Bezug auf Cybersicherheit unverzüglich austauschen. Diese Informationen würden zudem der ENISA helfen, ihre Aufgabe wahrzunehmen, die operative Zusammenarbeit zu unterstützen.

(35) Als Teil der regulären Zusammenarbeit auf technischer Ebene zur Unterstützung der EU-Lageeinschätzung sollte die ENISA auf der Grundlage öffentlich verfügbarer Informationen, ihrer eigenen Analysen und anhand von Berichten, die sie von den CSIRTs der Mitgliedstaaten oder den nationalen Anlaufstellen für die Sicherheit von Netz- und Informationssystemen gemäß der Richtlinie (EU) 2016/1148, in beiden Fällen auf freiwilliger Basis, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol und dem CERT-EU sowie gegebenenfalls dem EU-Zentrum für Informationsgewinnung und -analyse (EU INTCEN) des Europäischen Auswärtigen Dienstes erhalten hat, regelmäßig und in enger Zusammenarbeit mit den Mitgliedstaaten eingehende EU-Cybersicherheitslageberichte über Sicherheitsvorfälle und Bedrohungen erstellen. Dieser Bericht sollte dem Rat, der Kommission, der Hohen Vertreterin der Union für die Gemeinsame Außen- und Sicherheitspolitik und dem CSIRTs-Netz zur Verfügung gestellt werden.

(36) Die ENISA sollte sich bei der Unterstützung von nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen, die sie auf Ersuchen der betreffenden Mitgliedstaaten leistet, auf die Verhütung künftiger Sicherheitsvorfälle konzentrieren. Die betreffenden Mitgliedstaaten sollten die notwendigen Informationen und die erforderliche Hilfe bereitstellen, damit die ENISA die nachträgliche technische Untersuchung wirksam unterstützen kann.

([14]) ABl. C 12 vom 13.1.2018, S. 1.

([15]) Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

(37) Die Mitgliedstaaten können die von dem Sicherheitsvorfall betroffenen Unternehmen auffordern, mit der ENISA zusammenzuarbeiten und dieser — unbeschadet ihres Rechts, sensible Geschäftsinformationen und Informationen, die für die öffentliche Sicherheit von Bedeutung sind, zu schützen — die notwendigen Informationen und Hilfen zur Verfügung stellen.

(38) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union langfristige strategische Beratung anbieten zu können, muss die ENISA aktuelle und neu auftretende Cybersicherheitsrisiken analysieren. Hierzu sollte die ENISA in Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls Statistikämtern und anderen Stellen einschlägige öffentlich zugängliche oder freiwillig bereitgestellte Informationen sammeln und Analysen neu entstehender Technik sowie themenspezifische Bewertungen dazu durchführen, welche gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Folgen technische Innovationen für die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die ENISA sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union darüber hinaus bei der Ermittlung sich abzeichnender Cybersicherheitsrisiken und bei der Vermeidung von Vorfällen unterstützen, indem sie Analysen der Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle durchführt.

(39) Um die Abwehrfähigkeit der Union zu stärken, sollte die ENISA Fachwissen im Bereich der Cybersicherheit der Infrastrukturen, insbesondere zur Unterstützung der in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren und der Infrastrukturen, die von den in Anhang III jener Richtlinie aufgeführten Anbietern digitaler Dienste genutzt werden, aufbauen, indem Beratung, Leitlinien zur Verfügung gestellt und bewährte Verfahren ausgetauscht werden. Um den Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen zu erleichtern, sollte die ENISA das Informationsportal der Union aufbauen und pflegen, über das der Öffentlichkeit Informationen der Organe, Einrichtungen und sonstigen Stellen der Union und der Mitgliedstaaten zur Cybersicherheit bereitgestellt werden. Ein leichterer Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen könnte den Mitgliedstaaten auch dabei helfen, ihre Kapazitäten auszubauen und ihre Verfahren aufeinander abzustimmen, sodass die Abwehrfähigkeit gegenüber Cyberangriffen insgesamt gestärkt wird.

(40) Die ENISA sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, unter anderem durch eine unionsweite Sensibilisierungskampagne, die Förderung von Schulungen, und Leitlinien für bewährte Verfahren, die sich an Bürger, Organisationen und Unternehmen richten. Darüber hinaus sollte die ENISA einen Beitrag dazu leisten, bewährte Verfahren und Lösungen, einschließlich Cyberhygiene und Cyberkompetenz, auf der Ebene von Bürgern, Organisationen und Unternehmen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte und Leitlinien hierüber erstellt und veröffentlicht, die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit von Bürgern, Organisationen und Unternehmen insgesamt erhöhen. Die ENISA sollte sich außerdem bemühen, Verbrauchern relevante Informationen über anwendbare Zertifizierungsschemata an die Hand zu geben, indem sie beispielsweise Leitlinien und Empfehlungen bereitstellt. Ferner sollte die ENISA gemäß dem mit der Mitteilung der Kommission vom 17. Januar 2018 aufgestellten Aktionsplan für digitale Bildung in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten, um sicherere Verhaltensweisen der Nutzer im Internet und digitale Kompetenz zu fördern, die Nutzer stärker für potenzielle Bedrohungen im Internet — auch für die Internetkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug sowie Datenbetrug — zu sensibilisieren und einfache Empfehlungen in Bezug auf mehrstufige Authentifizierung, Patching, Verschlüsselung, Anonymisierung und Datenschutz zu geben.

(41) Die ENISA sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten und die sichere Nutzung von Diensten zu forcieren und auf Unionsebene konzeptionsintegrierte Sicherheit und konzeptionsintegrierten Schutz der Privatsphäre (privacy by design) zu fördern. Dabei sollte die ENISA die verfügbaren bewährten Verfahren und die vorhandene Erfahrung insbesondere von Forschungseinrichtungen und Wissenschaftlern im Bereich IT-Sicherheit optimal nutzen.

(42) Um die im Cybersicherheitssektor tätigen Unternehmen und die Nutzer von Cybersicherheitslösungen zu unterstützen, sollte die ENISA eine „Marktbeobachtungsstelle" aufbauen und pflegen, die die wichtigsten Nachfrage- und Angebotstrends auf dem Cybersicherheitsmarkt regelmäßig analysiert und bekannt macht.

(43) Die ENISA sollte einen Beitrag zu den Bemühungen der Union um eine Zusammenarbeit mit internationalen Organisationen sowie innerhalb der einschlägigen internationalen Gremien für die Zusammenarbeit im Bereich der Cybersicherheit leisten. Insbesondere sollte die ENISA gegebenenfalls an der Zusammenarbeit mit Organisationen wie der OECD, der OSZE und der NATO mitwirken. Diese Zusammenarbeit könnte gemeinsame Cybersicherheitsübungen und eine gemeinsame Koordinierung der Reaktion auf Sicherheitsvorfälle umfassen. Diese Aktivitäten müssen unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der Union — unbeschadet der spezifischen Merkmale der Sicherheits- und Verteidigungspolitik der einzelnen Mitgliedstaaten — erfolgen.

(44) Damit die ENISA ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Aufsichtsbehörden und anderen zuständigen Behörden in der Union und anderen zuständigen Behörden, Einrichtungen und sonstigen Stellen der Union Kontakt halten — etwa zum CERT-EU, EC3, zur Europäischen Verteidigungsagentur (EDA), zur Agentur für das Europäische zivile Satellitennavigationssystem (Europäische GNSS Agentur — GSA), zum Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Europäischen Zentralbank (EZB), zur Europäischen Bankenaufsichtsbehörde (EBA), zum Europäischen Datenschutzausschuss, zur Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER), zur Europäischen Agentur für Flugsicherheit (EASA) und zu sonstigen Agenturen der Union, die sich mit Fragen der Cybersicherheit beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Fragen der Cybersicherheit, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die ENISA auch mit diesen in Verbindung stehen. Vertreter der Strafverfolgungs- und der Datenschutzbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der ENISA-Beratungsgruppe in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsfragen, die sich möglicherweise auf deren Arbeit auswirken, sollte die ENISA vorhandene Informationskanäle und bestehende Netze beachten.

(45) Es könnten Partnerschaften mit Hochschulen eingerichtet werden, die in den einschlägigen Bereichen Forschungsinitiativen betreiben, und es sollten geeignete Kanäle für Beiträge von Verbraucherschutzverbänden und anderen Organisationen, die berücksichtigt werden sollten, zur Verfügung stehen.

(46) Die ENISA sollte in ihrer Rolle als Sekretariat des CSIRTs-Netzes bezüglich der in der Richtlinie (EU) 2016/1148 festgelegten einschlägigen Aufgaben des CSIRTs-Netzes die CSIRTs der Mitgliedstaaten und das CERT-EU bei der operativen Zusammenarbeit unterstützen. Zudem sollte die ENISA unter gebührender Berücksichtigung der Standardbetriebsverfahren des CSIRTs-Netzes die Zusammenarbeit zwischen den jeweiligen CSIRTs bei Sicherheitsvorfällen, Angriffen oder Störungen der von den CSIRTs verwalteten oder geschützten Netze oder Infrastrukturen, die mindestens zwei CSIRTs betreffen oder betreffen können, fördern und unterstützen.

(47) Zur Erhöhung der Abwehrbereitschaft der Union bei Cybersicherheitsvorfällen sollte die ENISA auf Unionsebene regelmäßige Cybersicherheitsübungen organisieren und die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union auf deren Ersuchen hin bei der Organisation solcher Übungen unterstützen. Eine Großübung sollte alle zwei Jahre veranstaltet werden, die technische, operative und strategische Elemente umfasst. Darüber hinaus sollte die ENISA regelmäßig weniger umfassende Übungen organisieren können, mit denen dasselbe Ziel verfolgt wird, nämlich die Abwehrbereitschaft der Union bei Sicherheitsvorfällen zu stärken.

(48) Die ENISA sollte ihre Sachkenntnis im Bereich der Cybersicherheitszertifizierung weiter ausbauen und pflegen, damit sie die Unionspolitik auf diesem Gebiet unterstützen kann. Die ENISA sollte auf bestehenden bewährten Verfahren aufbauen und die Nutzung der Cybersicherheitszertifizierung in der Union fördern, auch indem sie zum Aufbau und zur Pflege eines Rahmens für die Cybersicherheitszertifizierung auf Unionsebene (europäischer Rahmen für die Cybersicherheitszertifizierung) beiträgt, um so die Transparenz der Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt und in seine Wettbewerbsfähigkeit zu stärken.

(49) Effiziente Cybersicherheitsstrategien sollten sowohl im öffentlichen als auch im privaten Sektor auf sorgfältig entwickelten Risikobewertungsmethoden beruhen. Risikobewertungsmethoden werden auf verschiedenen Ebenen angewandt, ohne dass es eine einheitliche Vorgehensweise für deren effiziente Anwendung gibt. Durch die Förderung und Entwicklung bewährter Verfahren für die Risikobewertung und interoperabler Lösungen für das Risikomanagement innerhalb von Organisationen des öffentlichen und des privaten Sektors wird das Niveau der Cybersicherheit in der Union erhöht. Zu diesem Zweck sollte die ENISA die Zusammenarbeit zwischen Interessenträgern auf Unionsebene unterstützen und Hilfestellung bei deren Bemühungen um die Festlegung und Einführung von europäischen und internationalen Normen für das Risikomanagement und eine messbare Sicherheit in Bezug auf elektronische Produkte, Systeme, Netze und Dienste leisten, die im Zusammenwirken mit Software die Netz- und Informationssysteme bilden.

(50) Die ENISA sollte die Mitgliedstaaten, die Hersteller oder die Anbieter von IKT-Produkten, -Diensten oder -Prozessen dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können und sie sollte Anreize dazu geben. So sollten Hersteller und Anbieter von IKT-Produkten, -Diensten oder -Prozessen jegliche notwendigen Aktualisierungen bereitstellen und diese IKT-Produkte, -Dienste und -Prozesse zurückrufen, vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen, während Einführer und Händler sicherstellen sollten, dass IKT-Produkte, -Dienste und -Prozesse, die sie in der Union vermarkten, den geltenden Anforderungen genügen und kein Risiko für die Verbraucher in der Union darstellen.

(51) In Zusammenarbeit mit den zuständigen Behörden sollte die ENISA Informationen über das Niveau der Cybersicherheit von IKT-Produkten, -Diensten oder -Prozessen verbreiten, die auf dem Binnenmarkt angeboten werden, und sollte Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer IKT-Produkte, -Dienste oder -Prozesse zu verbessern.

(52) Die ENISA sollte die laufenden Tätigkeiten auf den Gebieten der Forschung, Entwicklung und technologischen Bewertung — insbesondere die im Rahmen der vielfältigen Forschungsinitiativen der Union durchgeführten Tätigkeiten — umfassend berücksichtigen, um die Organe, Einrichtungen und sonstigen Stellen der Union sowie gegebenenfalls die Mitgliedstaaten — auf deren Ersuchen — in Bezug auf den Forschungsbedarf und die Prioritäten im Bereich der Cybersicherheit zu beraten. Um den Bedarf und die Prioritäten im Forschungsbereich zu ermitteln, sollte die ENISA auch die einschlägigen Nutzergruppen konsultieren. Insbesondere könnte eine Zusammenarbeit mit dem Europäischen Forschungsrat und dem Europäischen Innovations- und Technologieinstitut sowie mit dem Institut der Europäischen Union für Sicherheitsstudien eingerichtet werden.

(53) Die ENISA sollte die Normungsgremien, insbesondere die europäischen Normungsgremien, bei der Ausarbeitung von europäischen Schemata für die Cybersicherheitszertifizierung regelmäßig konsultieren.

(54) Cyberbedrohungen bestehen weltweit. Um die Cybersicherheitsstandards, einschließlich der Notwendigkeit der Festlegung gemeinsamer Verhaltensnormen und der Annahme von Verhaltenskodizes, der Verwendung internationaler Normen und des Informationsaustauschs zu verbessern sowie eine zügigere internationale Zusammenarbeit bei der Abwehr und einen weltweiten gemeinsamen Ansatz für Probleme der Netz- und Informationssicherheit zu fördern, bedarf es einer engeren internationalen Zusammenarbeit. In dieser Hinsicht sollte die ENISA ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt.

(55) Die ENISA sollte in der Lage sein, auf Ersuchen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der Union um Rat und Hilfestellung zu Angelegenheiten, die durch das Mandat der ENISA abgedeckt sind, ad hoc zu reagieren.

(56) In Bezug auf die Führung der ENISA ist es vernünftig und wird empfohlen bestimmte Prinzipien umzusetzen, um der Gemeinsamen Erklärung und dem Gemeinsamen Konzept zu entsprechen, die von der Interinstitutionellen Arbeitsgruppe zu den dezentralen Einrichtungen der EU im Juli 2012 vereinbart wurden und deren Zweck darin besteht, die Aktivitäten der dezentralen Agenturen dynamischer zu gestalten und ihre Leistung zu verbessern. Die in der Gemeinsamen Erklärung und dem Gemeinsamen Konzept enthaltenen Empfehlungen sollten gegebenenfalls auch in den Arbeitsprogrammen, den Bewertungen und den Berichterstattungs- und Verwaltungsverfahren der ENISA zur Geltung kommen.

(57) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, sollte die allgemeine Ausrichtung der Tätigkeit der ENISA festlegen und dafür sorgen, dass sie ihre Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte über die erforderlichen Befugnisse verfügen, um den Haushaltsplan zu erstellen und die Ausführung des Haushaltsplans zu überprüfen, angemessene Finanzvorschriften und transparente Verfahren für die Entscheidungsfindung der ENISA festzulegen, das einheitliche Programmplanungsdokument der ENISA anzunehmen, sich eine Geschäftsordnung zu geben, den Exekutivdirektor zu ernennen und über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen.

(58) Damit die ENISA ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und geeignete Erfahrung verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.

(59) Damit die ENISA reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird und über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt. Die Aufgaben des Exekutivdirektors sollten in völliger Unabhängigkeit wahrgenommen werden. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das jährliche Arbeitsprogramm der ENISA ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen dem Verwaltungsrat vorzulegenden Jahresbericht, in dem auch die Umsetzung des jährlichen Arbeitsprogramms der ENISA behandelt wird, ausarbeiten, einen Entwurf eines Voranschlags für die Einnahmen und Ausgaben der ENISA erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder sozioökonomischen Einzelfragen befassen. Insbesondere im Zusammenhang mit der Ausarbeitung eines möglichen europäischen Schemas für die Cybersicherheitszertifizierung (im Folgenden „mögliches Schema“) wird die Einrichtung einer Ad-hoc-Arbeitsgruppe für notwendig

erachtet. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen, ein ausgewogenes Verhältnis von Frauen und Männern besteht und dass je nach behandelter Einzelfrage gegebenenfalls ein angemessenes Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit gewahrt wird.

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

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

(62) Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte eingesetzt werden, um der ENISA und der Kommission die Konsultation der maßgeblichen Interessenträger zu erleichtern. Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte sich in ausgewogenem Verhältnis aus Branchenvertretern sowohl der Nachfrage- als auch der Angebotsseite in Bezug auf IKT-Produkte und -Dienste zusammensetzen; insbesondere sollten KMU, Anbieter digitaler Dienste, europäische und internationale Normungsgremien, nationale Akkreditierungsstellen, Datenschutz-Aufsichtsbehörden, Konformitätsbewertungsstellen gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([16]) und die Wissenschaft sowie Verbraucherorganisationen vertreten sein.

(63) Die ENISA sollte über Vorschriften zur Vermeidung und Handhabung von Interessenkonflikten verfügen. Die ENISA sollte die einschlägigen Bestimmungen der Union in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([17]) anwenden. Die Verarbeitung personenbezogener Daten durch die ENISA sollte nach der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([18]) erfolgen. Die ENISA sollte die für die Organe, Einrichtungen und sonstigen Stellen der Union geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der Europäischen Union (EUCI), sowie die entsprechenden nationalen Rechtsvorschriften befolgen.

(64) Damit die volle Autonomie und Unabhängigkeit der ENISA gewährleistet ist und sie zusätzliche Aufgaben — auch nicht vorhergesehene Aufgaben in Notfällen — erfüllen kann, sollte die ENISA über einen ausreichenden und eigenständigen Haushalt verfügen, der hauptsächlich durch einen Beitrag der Union und durch Beiträge von Drittländern, die sich an der Arbeit der ENISA beteiligen, finanziert werden sollte. Ein angemessen ausgestatteter Haushaltsplan ist von entscheidender Bedeutung dafür, dass die ENISA ausreichende Kapazitäten hat, um ihren wachsenden Aufgaben zu erfüllen und ihre Ziele zu erreichen. Die Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der ENISA befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zum Haushaltsplan der ENISA zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der ENISA durch den Rechnungshof geprüft werden, um Transparenz und Rechenschaftspflicht sicherzustellen.

(65) Die Cybersicherheitszertifizierung spielt eine große Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte, Dienste und Prozesse ein gewisses Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie und intelligente Netze sind, sind nur einige Beispiele von Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die Richtlinie (EU) 2016/1148 fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

([16]) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

([17]) Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

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

(66) In ihrer Mitteilung aus dem Jahr 2016 mit dem Titel „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“ unterstrich die Kommission die Notwendigkeit hochwertiger, erschwinglicher und interoperabler Produkte und Lösungen für die Cybersicherheit. Allerdings ist das Angebot an IKT-Produkten, -Diensten und -Prozessen im Binnenmarkt nach wie vor geografisch stark zersplittert. Das liegt daran, dass sich die Cybersicherheitsbranche in Europa überwiegend aufgrund der Nachfrage der nationalen Regierungen entwickelt hat. Zudem gehört der Mangel an interoperablen Lösungen (technischen Normen), Verfahrensweisen und unionsweiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. Dies macht es für europäische Unternehmen schwerer, im nationalen, unionsweiten und weltweiten Wettbewerb zu bestehen. Es verringert sich dadurch auch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen können. Auch in der Mitteilung des Jahres 2017 zur Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt — Ein vernetzter digitaler Binnenmarkt für alle — unterstrich die Kommission die Bedeutung sicherer vernetzter Produkte und Systeme und verwies darauf, dass die Schaffung eines europäischen Rahmens für die IKT-Sicherheit, auf dessen Grundlage Vorschriften für die Organisation der IKT-Sicherheitszertifizierung in der Union festgelegt werden, dafür sorgen kann, dass das Vertrauen in den Binnenmarkt erhalten bleibt und die derzeitige Fragmentierung des Binnenmarkts eingedämmt wird.

(67) Derzeit werden IKT-Produkte, -Dienste und -Prozesse, im Hinblick auf ihre Cybersicherheit kaum zertifiziert. Wenn dies doch der Fall ist, geschieht es meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Behörde für die Cybersicherheitszertifizierung ausgestelltes Zertifikat nicht grundsätzlich auch in anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre IKT-Produkte, -Dienste und -Prozesse möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen, was ihre Kosten erhöht. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf, was die Verfahren zur gegenseitigen Anerkennung in der Union behindert.

(68) Einige Anstrengungen wurden bereits unternommen, um eine gegenseitige Anerkennung der Zertifikate in der Union zu gewährleisten. Diese waren jedoch nur zum Teil erfolgreich. Das in dieser Hinsicht wichtigste Beispiel ist die in der Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) getroffene Vereinbarung über die gegenseitige Anerkennung (MRA). Auch wenn diese Vereinbarung das wichtigste Vorbild für die Zusammenarbeit und gegenseitige Anerkennung auf dem Gebiet der Sicherheitszertifizierung ist, umfasst die SOG-IS nur einige der Mitgliedstaaten. Dies hat aus Binnenmarktsicht zur Folge, dass die Vereinbarungen der Gruppe nur begrenzt wirksam sind.

(69) Daher ist es notwendig, einen gemeinsamen Ansatz zu verfolgen und einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Schemata für die Cybersicherheitszertifizierung festgelegt werden, damit die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen für IKT-Produkte, -Dienste oder -Prozesse in allen Mitgliedstaaten anerkannt und verwendet werden können. Dabei ist es wichtig, auf vorhandenen nationalen und internationalen Schemata sowie auf Systemen der gegenseitigen Anerkennung, insbesondere der SOG-IS, aufzubauen und einen reibungslosen Übergang von vorhandenen Schemata im Rahmen solcher Systeme zu Schemata auf der Grundlage des neuen europäischen Rahmens für die Cybersicherheitszertifizierung zu ermöglichen. Mit einem europäischen Rahmen für die Cybersicherheitszertifizierung sollten zwei Ziele verfolgt werden: erstens sollte er dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu erhöhen, die nach Schemata für die europäische Cybersicherheitszertifizierung zertifiziert wurden. Zweitens sollte er dazu beitragen, dass sich vielfältige, sich widersprechende oder überlappende nationale Schemata für die Cybersicherheitszertifizierung vermeiden lassen, und so die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senken. Die europäischen Schemata für die Cybersicherheitszertifizierung sollten nichtdiskriminierend sein und sich auf europäische oder internationale Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der Union in diesem Bereich sind.

(70) Der europäische Rahmen für die Cybersicherheitszertifizierung sollte in einheitlicher Weise in allen Mitgliedstaaten eingeführt werden, damit es nicht aufgrund unterschiedlicher Anforderungsniveaus zwischen den Mitgliedstaaten zu einem „Zertifizierungsshopping“ kommt.

(71) Europäische Schemata für die Cybersicherheitszertifizierung sollten auf dem auf internationaler und nationaler Ebene bereits Vorhandenen und erforderlichenfalls auf den von Gremien und Konsortien erstellten technischen Spezifikationen aufbauen, wobei die derzeitigen Stärken genutzt und Schwachstellen bewertet und behoben werden sollten.

(72) Es bedarf flexibler Cybersicherheitslösungen, damit die Branche den Cyberbedrohungen immer einen Schritt voraus ist und daher sollte jedes Zertifizierungsschema so gestaltet werden, dass das Risiko eines schnellen Veraltens vermieden wird.

(73) Die Kommission sollte befugt sein, für bestimmte Gruppen von IKT-Produkten, -Diensten und -Prozessen europäische Schemata für die Cybersicherheitszertifizierung anzunehmen. Diese Schemata sollten von nationalen Behörden für die Cybersicherheitszertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Schemata erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungsschemata sollten nicht in den Anwendungsbereich dieser Verordnung fallen. Die Stellen, die solche Schemata betreiben, sollten der Kommission jedoch vorschlagen können, ihre Systeme als Grundlage für ein europäisches Schema für die Cybersicherheitszertifizierung in Betracht zu ziehen und sie als ein solches zu genehmigen.

(74) Die Rechtsvorschriften der Union, in denen bestimmte Vorschriften zur Zertifizierung von IKT-Produkten, -Diensten und -Prozessen festgelegt sind, bleiben von den Bestimmungen dieser Verordnung unberührt. Insbesondere enthält die Verordnung (EU) 2016/679 Bestimmungen zur Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der genannten Verordnung einhalten. Solche Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen sollten den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger IKT-Produkte, -Dienste und -Prozesse ermöglichen. Die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Verordnung (EU) 2016/679 fallen, auch wenn solche Vorgänge in IKT-Produkte, -Dienste und -Prozesse eingebettet sind, bleibt von der vorliegenden Verordnung unberührt.

(75) Mit den europäischen Schemata für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte, -Dienste und -Prozesse bestimmten Anforderungen genügen, deren Ziel es ist, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte, -Dienste und -Prozesse im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte, -Dienste und -Prozesse und der damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit zu entwickeln, die unter allen Umständen gültig sind. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, das durch besondere Cybersicherheitsziele ergänzt werden sollte, die bei der Konzeption der europäischen Schemata für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte, -Dienste und -Prozesse erreicht werden sollen, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungsschemas festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen, wenn keine angemessenen Normen verfügbar sind.

(76) Die in europäischen Schemata für die Cybersicherheitszertifizierung zu verwendenden technischen Spezifikationen sollten unter Beachtung der in Anhang II der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([19]) festgelegten Anforderungen bestimmt werden. Gewisse Abweichungen von diesen Anforderungen könnten jedoch in hinreichend begründeten Fällen als notwendig erachtet werden, wenn diese technischen Spezifikationen in einem europäischen Schema für die Cybersicherheitszertifizierung in der Vertrauenswürdigkeitsstufe „hoch" verwendet werden sollen. Die Gründe für solche Abweichungen sollten öffentlich zugänglich gemacht werden.

(77) Eine Konformitätsbewertung ist ein Verfahren, mit dem bewertet wird, ob bestimmte Anforderungen an ein IKT-Produkt, einen IKT-Dienst oder einen IKT-Prozess erfüllt werden. Dieses Verfahren wird von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller oder den Anbieter der IKT-Produkte, -Dienste oder -Prozesse, welche bewertet werden, handelt, durchgeführt. Ein europäisches Cybersicherheitszertifikat sollte nach der erfolgreichen Bewertung eines IKT-Produkts, -Dienstes oder -Prozesses ausgestellt werden. Ein europäisches Cybersicherheitszertifikat sollte als Bestätigung gelten, dass die Bewertung ordnungsgemäß durchgeführt wurde. Je nach Vertrauenswürdigkeitsstufe sollte im europäischen Schema für die Cybersicherheitszertifizierung angegeben werden, ob ein europäisches Cybersicherheitszertifikat von einer privaten oder einer öffentlichen Stelle auszustellen ist. Die Konformitätsbewertung und die Zertifizierung an sich können nicht garantieren, dass die zertifizierten IKT-Produkte, -Dienste und -Prozesse cybersicher sind. Es handelt sich vielmehr um Verfahren und technische Methoden, um zu bescheinigen, dass die IKT-Produkte, -Dienste und -Prozesse geprüft wurden und bestimmte Anforderungen an die Cybersicherheit erfüllen, wie sie anderweitig, beispielsweise in technischen Normen, festgelegt sind.

(78) Die Auswahl der angemessenen Zertifizierung und der dazugehörigen Sicherheitsanforderungen durch die Nutzer der europäischen Cybersicherheitszertifizierung sollte auf der Grundlage einer Risikoanalyse der Verwendung des IKT-Produkts, -Dienstes oder -Prozesses erfolgen. Dementsprechend sollte die Vertrauenswürdigkeitsstufe das mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundene Risiko widerspiegeln.

([19]) 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).

(79) Europäische Schemata für die Cybersicherheitszertifizierung könnten eine Konformitätsbewertung vorsehen, die unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen durchzuführen wäre (im Folgenden „Selbstbewertung der Konformität"). In diesen Fällen sollte es ausreichen, dass der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen selbst alle Überprüfungen vornimmt, um sicherzustellen, dass die IKT-Produkte, -Dienste oder -Prozesse mit dem europäischen Schema für die Cybersicherheitszertifizierung konform sind. Die Selbstbewertung der Konformität sollte für IKT-Produkte, -Dienste oder -Prozesse von geringer Komplexität, die ein geringes Risiko für die Öffentlichkeit darstellen, wie bei einfacher Konzeption und einfachem Herstellungsmechanismus, als angemessen angesehen werden. Zudem sollte die Selbstbewertung der Konformität nur dann für IKT-Produkte, IKT-Dienste oder IKT-Prozesse erlaubt sein, wenn sie der Vertrauenswürdigkeitsstufe „niedrig" entsprechen.

(80) Europäische Schemata für die Cybersicherheitszertifizierung könnten sowohl die Selbstbewertung der Konformität als auch die Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen zulassen. In einem solchen Fall sollten im System klare und verständliche Instrumente für Verbraucher oder andere Nutzer vorgesehen werden, mit denen sie zwischen IKT-Produkten, -Diensten oder -Prozessen, die unter der Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen bewertet werden, und IKT-Produkten, -Diensten oder -Prozessen, die von einem Dritten zertifiziert werden, unterscheiden können.

(81) Ein Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, der eine Selbstbewertung der Konformität durchführt, sollte die EU-Konformitätserklärung im Rahmen des Konformitätsbewertungsverfahrens abfassen und unterzeichnen können. Eine EU-Konformitätserklärung ist ein Dokument, welches bestätigt, dass das betreffende IKT-Produkt, der betreffende IKT-Dienst oder der betreffende IKT-Prozess die Anforderungen des Schemas erfüllt. Durch die Abfassung und Unterzeichnung der EU-Konformitätserklärung übernimmt der Hersteller oder Anbieter die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess die rechtlichen Anforderungen des europäischen Schemas für die Cybersicherheitszertifizierung erfüllt. Eine Kopie der EU-Konformitätserklärung sollte der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorgelegt werden.

(82) Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen sollten die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, -Dienste oder -Prozesse mit einem System während eines Zeitraums, der im einschlägigen europäischen Schema für die Cybersicherheitszertifizierung festgelegt ist, für die zuständige nationale Behörde für die Cybersicherheitszertifizierung bereithalten. In der technischen Dokumentation sollten die in diesem System geltenden Anforderungen aufgeführt werden und die Konzeption, Herstellung und Funktionsweise des IKT-Produkts, -Dienstes oder -Prozesses erfasst werden. Die technische Dokumentation sollte so erstellt werden, dass es möglich ist, die Konformität eines IKT-Produkts oder -Dienstes mit den in diesem System geltenden Anforderungen zu bewerten.

(83) Bei der Gestaltung des Rahmens des europäischen Schemas für die Cybersicherheitszertifizierung sollte die Einbeziehung der Mitgliedstaaten sowie eine angemessene Einbeziehung der Interessenträger berücksichtigt werden; ferner sollte die Rolle der Kommission während der Planung und Vorlage eines europäischen Schemas für die Cybersicherheitszertifizierung, der Erteilung des entsprechenden Auftrags sowie der Ausarbeitung, der Annahme und der Überprüfung eines europäischen Schemas für die Cybersicherheitszertifizierung festgelegt werden.

(84) Die Kommission sollte mit Unterstützung der Europäischen Gruppe für die Cybersicherheitszertifizierung und der Gruppe der Interessenträger für die Cybersicherheitszertifizierung im Anschluss an eine offene und umfassende Konsultation ein fortlaufendes Arbeitsprogramm der Union für europäische Schemata für die Cybersicherheitszertifizierung ausarbeiten und in Form eines nicht verbindlichen Instruments veröffentlichen. Das fortlaufende Arbeitsprogramm der Union sollte ein strategisches Dokument sein und insbesondere der Branche, den nationalen Behörden und den Normungsgremien ermöglichen, sich auf die künftigen Europäischen Schemata für die Cybersicherheitszertifizierung vorzubereiten. Das fortlaufende Arbeitsprogramm der Union sollte eine mehrjährige Übersicht über die Aufträge für die Ausarbeitung möglicher Systeme umfassen, die die Kommission der ENISA aus bestimmten Gründen zu erteilen beabsichtigt. Die Kommission sollte dieses fortlaufende Arbeitsprogramm der Union im Rahmen des fortlaufenden Plans für die IKT-Normung und bei der Erstellung ihrer Normungsaufträge an die europäischen Normungsorganisationen berücksichtigen. Wegen der raschen Einführung und Übernahme neuer Technologien sowie die Entstehung bislang unbekannter Cybersicherheitsrisiken und Gesetzgebungs- und Marktentwicklungen sollte die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungsschemata, die nicht im fortlaufenden Arbeitsprogramm der Union enthalten waren, zu beauftragen. In solchen Fällen sollten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung auch die Notwendigkeit eines solchen Auftrags bewerten, wobei die allgemeinen Zielsetzungen und Vorgaben dieser Verordnung und die Notwendigkeit der Kontinuität bei der Planung der ENISA und der Nutzung der Ressourcen durch die ENISA zu berücksichtigen sind.

Im Anschluss an einen solchen Auftrag sollte die ENISA ohne ungebührliche Verzögerung mögliche Zertifizierungsschemata für bestimmte IKT- Produkte -Dienste und -Prozesse, ausarbeiten. Die Kommission sollte die positiven und negativen Auswirkungen ihres Auftrags auf den spezifischen Markt und insbesondere auf KMU, Innovation, die Schranken für den Eintritt in diesen Markt und die Kosten für die Endverbraucher bewerten. Die Kommission sollte befugt sein, auf der Grundlage des von der ENISA vorbereiteten möglichen Schemas das europäische Schema für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks dieser Verordnung und der in ihr festgelegten Sicherheitsziele sollten in den von der Kommission angenommenen europäischen Schemata für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Schemas festgelegt werden. Unter diese Bestimmungen sollte unter anderem Folgendes fallen: Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten, -Diensten und -Prozessen, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe („niedrig“, „mittel“ oder „hoch“) sowie gegebenenfalls die Bewertungsniveaus. Die ENISA sollte einen Auftrag der Europäischen Gruppe für die Cybersicherheitszertifizierung ablehnen können. Solche Entscheidungen sollten gebührend begründet und vom Verwaltungsrat getroffen werden.

(85) Die ENISA sollte eine eigene Website unterhalten, auf der sie über die europäischen Schemata für die Cybersicherheitszertifizierung informiert und für diese wirbt und auf der unter anderem die Aufträge für die Ausarbeitung eines möglichen Schemas und die Rückmeldungen im Rahmen des Konsultationsverfahrens, das von der ENISA in der Ausarbeitungsphase durchgeführt wird, zur Verfügung stehen. Auf der Website sollten auch Informationen über die europäischen Cybersicherheitszertifikate und die nach dieser Verordnung ausgestellten EU-Konformitätserklärungen einschließlich Informationen zum Widerruf und Ablauf solcher europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bereitgestellt werden. Auf der Website sollten auch diejenigen nationalen Schemata für die Cybersicherheitszertifizierung angegeben werden, die durch ein europäisches Schema für die Cybersicherheitszertifizierung ersetzt wurden.

(86) Die Vertrauenswürdigkeit eines europäischen Zertifizierungsschemas ist die Grundlage für das Vertrauen, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines spezifischen europäischen Schemas für die Cybersicherheitszertifizierung genügt. Um die Kohärenz des Rahmens für ein europäisches Schema für die Cybersicherheitszertifizierung zu gewährleisten, sollte ein europäisches Schema für die Cybersicherheitszertifizierung die Vertrauenswürdigkeitsstufen für europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, die im Rahmen dieses Schemas ausgestellt werden, angeben können. Jedes europäische Cybersicherheitszertifikat könnte sich auf eine der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ beziehen, wohingegen sich die EU-Konformitätserklärung nur auf die Vertrauenswürdigkeitsstufe „niedrig“ beziehen könnte. Die Vertrauenswürdigkeitsstufen würden die entsprechende Strenge und Gründlichkeit für die Bewertung des IKT-Produkts, -Dienstes oder -Prozesses vorgeben und durch Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Vorfällen besteht, gekennzeichnet sein. Jede Vertrauenswürdigkeitsstufe sollte in den verschiedenen Bereichen der Sektoren, in denen die Zertifizierung angewandt wird, einheitlich sein.

(87) In einem europäischen Schema für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der verwendeten Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden. Die Evaluierungsstufen sollten jeweils einer der Vertrauenswürdigkeitsstufen entsprechen und mit einer entsprechenden Kombination von Vertrauenswürdigkeitskomponenten verknüpft sein sollten. Für alle Vertrauenswürdigkeitsstufen sollte das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess eine Reihe sicherer Funktionen enthalten, die im jeweiligen System festgelegt sind, so unter anderem eine voreingestellte sichere Konfiguration, einen signierten Code, ein sicheres Aktualisierungsverfahren und die Reduzierung von Exploits sowie eine vollständige Absicherung von Stapelspeicher (Stack) oder dynamischem Speicher (Heap). Diese Funktionen sollten weiterentwickelt und gepflegt werden, wobei sicherheitsorientierte Entwicklungskonzepte und dazugehörige Instrumente zu verwenden sind, um sicherzustellen, dass wirksame Software- und Hardware-Mechanismen zuverlässig integriert werden.

(88) Bei der Vertrauenswürdigkeitsstufe „niedrig“ sollte sich die Bewertung mindestens auf die folgenden Vertrauenswürdigkeitskomponenten stützen: Die Bewertung sollte mindestens eine Überprüfung der technischen Dokumentation des IKT-Produkts -Dienstes oder -Prozesses durch die Konformitätsbewertungsstelle umfassen. Schließt die Zertifizierung IKT-Prozesse ein, sollte auch das Verfahren zur Konzipierung, Entwicklung und Pflege eines IKT-Produkts oder -Dienstes einer technischen Überprüfung unterzogen werden. Ist in einem europäischen Schema für die Cybersicherheitszertifizierung eine Selbstbewertung der Konformität vorgesehen, so sollte es genügen, wenn der Hersteller oder Anbieter von IKT- Produkten, Diensten oder Prozessen eine Selbstbewertung der Konformität des IKT-Produkts, -Dienstes oder -Prozesses, mit dem Zertifizierungsschema vornimmt.

(89) Bei der Vertrauenswürdigkeitsstufe „mittel“ sollte sich die Bewertung — zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „niedrig“ — mindestens auf eine Überprüfung der Konformität der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses mit seiner technischen Dokumentation stützen.

(90) Bei der Vertrauenswürdigkeitsstufe „hoch“ sollte sich die Bewertung — zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „mittel“ — mindestens auf einen Wirksamkeitstest stützen, bei dem die Widerstandsfähigkeit der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses gegen gründlich vorbereitete Cyberattacken bewertet wird, die von Akteuren mit umfangreichen Fähigkeiten und Ressourcen durchgeführt wird.

(91) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung und eine EU-Konformitätserklärung sollte freiwillig bleiben, sofern im Unionsrecht oder in entsprechend dem Unionsrecht erlassenen Rechtsvorschriften der Mitgliedstaaten nichts anderes festgelegt ist. Falls es keine harmonisierten Unionsrechtsvorschriften gibt, können die Mitgliedstaaten nationale technische Vorschriften gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([20]) erlassen. Die Mitgliedstaaten können auch im Zusammenhang mit öffentlichen Ausschreibungen und der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates ([21]) auf eine europäische Cybersicherheitszertifizierung zurückgreifen.

(92) In einigen Bereichen könnte es künftig notwendig werden, bestimmte Anforderungen an die Cybersicherheit und die entsprechende Zertifizierung für bestimmte IKT-Produkte, -Dienste oder -Prozesse verbindlich vorzuschreiben, um das Niveau der Cybersicherheit in der Union zu erhöhen. Die Kommission sollte die Auswirkungen der angenommenen europäischen Schemata für die Cybersicherheitszertifizierung auf die Verfügbarkeit sicherer IKT-Produkte, -Dienste und -Prozesse im Binnenmarkt regelmäßig überwachen und sollte regelmäßig bewerten, inwieweit die Zertifizierungsschemata durch die Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen in der Union genutzt werden. Die Effizienz der europäischen Schemata für die Cybersicherheitszertifizierung und die Frage, ob bestimmte Systeme verbindlich vorgeschrieben werden sollten, sollte anhand der Rechtsvorschriften der Union im Bereich der Cybersicherheit, insbesondere der Richtlinie (EU) 2016/1148, unter Berücksichtigung der Sicherheit der von Betreibern wesentlicher Dienste genutzten Netz- und Informationssysteme bewertet werden.

(93) Die europäischen Cybersicherheitszertifikate und die EU-Konformitätserklärung sollten den Endnutzern dabei helfen, kundige Entscheidungen zu treffen. Daher sollten IKT-Produkte, -Dienste und -Prozesse, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, strukturierte Informationen beigegeben werden, die an das erwartete technische Niveau des vorgesehenen Endnutzers angepasst sind. Alle diese Informationen sollten online verfügbar sein, und gegebenenfalls physisch bereitgestellt werden. Der Endnutzer sollte Zugang zu Informationen über die Kennnummer des Zertifizierungsschemas, die Vertrauenswürdigkeitsstufe, die Beschreibung der Cybersicherheitsrisiken in Verbindung mit dem IKT-Produkt, -Dienst oder -Prozess sowie die ausstellende Stelle haben oder eine Kopie des europäischen Cybersicherheitszertifikats erhalten können. Darüber hinaus sollten die Endnutzer über die Politik des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Förderung der Cybersicherheit, d. h. darüber, wie lange ein Endnutzer Aktualisierungen oder Patches im Bereich der Cybersicherheit erwarten kann, informiert sein. Gegebenenfalls sollten Leitlinien über Maßnahmen oder Einstellungen, die der Endnutzer von IKT-Produkten oder -Diensten zur Aufrechterhaltung oder Verbesserung der Cybersicherheit vornehmen kann, und Kontaktinformationen einer zentralen Anlaufstelle zur Meldung von Cyberangriffen und zur Unterstützung im Fall von Cyberangriffen (neben der automatischen Berichterstattung) zur Verfügung gestellt werden. Diese Informationen sollten regelmäßig auf den neuesten Stand gebracht werden und auf einer Website, die Informationen über das europäische Schema für die Cybersicherheitszertifizierung bereitstellt, zur Verfügung stehen.

(94) Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Schemata oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte, -Dienste oder -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab einem Zeitpunkt unwirksam werden, den die Kommission in Durchführungsrechtsakten festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Schemata für die Cybersicherheitszertifizierung der IKT-Produkte, -Dienste oder -Prozesse einführen, die bereits unter ein geltendes europäisches Schema für die Cybersicherheitszertifizierung fallen. Allerdings sollte es den Mitgliedstaaten freistehen, aus Gründen der nationalen Cybersicherheit nationale Cyberzertifizierungsschemata einzuführen oder beizubehalten. Die Mitgliedstaaten sollten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung über ihre Absicht unterrichten, neue nationale Schemata für die Cybersicherheitszertifizierung auszuarbeiten. Die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung sollten die Auswirkungen des neuen nationalen Schemas für die Cybersicherheitszertifizierung auf das ordnungsgemäße Funktionieren des Binnenmarkts und im Hinblick auf das strategische Interesse bewerten, stattdessen einen Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung zu erteilen.

(95) Die europäischen Schemata für die Cybersicherheitszertifizierung sollen dabei helfen, die Cybersicherheitsverfahren in der Union zu harmonisieren. Sie müssen dazu beitragen, das Niveau der Cybersicherheit in der Union zu erhöhen. Das Design der europäischen Schemata für die Cybersicherheitszertifizierung sollte weitere Innovationen im Bereich der Cybersicherheit berücksichtigen und ermöglichen werden.

([20]) 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.)

([21]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

(96) Die europäischen Schemata für die Cybersicherheitszertifizierung sollten die derzeitigen Methoden der Software- und Hardware-Entwicklung und insbesondere die Auswirkungen häufiger Software- oder Firmware-Aktualisierungen zu einzelnen europäischen Cybersicherheitszertifikaten berücksichtigen. Bei den europäischen Schemata für die Cybersicherheitszertifizierung sollten die Bedingungen angegeben werden, unter denen eine Aktualisierung erfordern kann, dass ein IKT-Produkt, ein IKT-Dienst oder ein IKT-Prozess neu zertifiziert werden muss oder dass der Umfang des spezifischen europäische Cybersicherheitszertifikats eingeschränkt werden muss, wobei die möglichen nachteiligen Auswirkungen der Aktualisierung auf die Einhaltung der Sicherheitsanforderungen des Zertifikats zu berücksichtigen sind.

(97) Sobald ein europäisches Schema für die Cybersicherheitszertifizierung eingeführt worden ist, sollten die Hersteller oder die Anbieter von IKT-Produkten, -Diensten oder -Prozessen die Zertifizierung ihrer IKT-Produkte, -Dienste oder -Prozesse bei einer nationalen Konformitätsbewertungsstelle ihrer Wahl an einem beliebigen Ort in der Union beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer nationalen Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen weiterhin erfüllt. Die nationalen Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung beschränken, aussetzen oder widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht erfüllt wurden oder nicht mehr erfüllt werden oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

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

(99) Zur Erreichung gleichwertiger Standards in der gesamten Union, zur Erleichterung der gegenseitigen Anerkennung und zur Förderung der allgemeinen Akzeptanz der Europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bedarf es eines Systems der gegenseitigen Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung. Die gegenseitige Begutachtung sollte Verfahren für Folgendes umfassen: Überwachung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den europäischen Cybersicherheitszertifikaten, Überwachung der Verpflichtungen der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen, die eine Selbstbewertung der Konformität vornehmen, Überwachung der Konformitätsbewertungsstellen sowie Angemessenheit des Fachwissens des Personals der Einrichtungen, die Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Die Kommission sollte im Wege von Durchführungsrechtsakten mindestens einen Fünfjahresplan für gegenseitige Begutachtungen sowie Kriterien und Methoden für die Abwicklung der gegenseitigen Begutachtungen festlegen können.

(100) Unbeschadet des allgemeinen Systems der gegenseitigen Begutachtung, das zwischen allen nationalen Behörden für die Cybersicherheitszertifizierung im Rahmen der europäischen Cybersicherheitszertifizierung eingerichtet werden soll, können bestimmte Schemata für die europäische Cybersicherheit ein Verfahren zur gegenseitigen Begutachtung der Stellen für die Ausstellung europäischer Cybersicherheitszertifikate für IKT-Produkte, -Dienste und -Prozesse auf der Vertrauenswürdigkeitsstufe „hoch“ im Rahmen solcher Schemata umfassen. Die Gruppe für die Cybersicherheitszertifizierung sollte die Umsetzung der Verfahren der gegenseitigen Begutachtung unterstützen. Bei solchen gegenseitigen Begutachtungen sollte insbesondere bewertet werden, ob die betreffenden Stellen ihre Aufgaben einheitlich ausführen; zudem können sie Einspruchsmöglichkeiten umfassen. Die Ergebnisse der gegenseitigen Begutachtungen sollten veröffentlicht werden. Die betreffenden Stellen können entsprechend geeignete Maßnahmen ergreifen, um ihre Verfahren und Sachkenntnisse anzupassen.

(101) Die Mitgliedstaaten sollten eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung benennen, die die Einhaltung der sich aus dieser Verordnung ergebenden Verpflichtungen beaufsichtigen. Eine nationale Behörde für die Cybersicherheitszertifizierung kann eine bereits bestehende oder eine neue Behörde sein. Ein Mitgliedstaat sollte im gegenseitigen Einvernehmen mit einem anderen Mitgliedstaat auch eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung im Hoheitsgebiet dieses anderen Mitgliedstaats benennen können.

(102) Die nationalen Behörden für die Cybersicherheitszertifizierung sollten insbesondere die Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen in Bezug auf die EU-Konformitätserklärung überwachen und durchsetzen, die nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen durch Bereitstellung von Sachkenntnis und einschlägigen Informationen unterstützen, Konformitätsbewertungsstellen ermächtigen, ihre Aufgaben wahrzunehmen, wenn diese in einem europäischen Schema für die Cybersicherheitszertifizierung festgelegte zusätzliche Anforderungen erfüllen, und einschlägige Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung verfolgen. Die nationalen Behörden für die Cybersicherheitszertifizierung sollten auch Beschwerden bearbeiten, die von natürlichen oder juristischen Personen in Bezug auf die von diesen Behörden ausgestellten europäischen Cybersicherheitszertifikate oder die in Verbindung mit den europäischen Cybersicherheitszertifikaten von Konformitätsbewertungsstellen ausgestellten Zertifikate für die Vertrauenswürdigkeitsstufe

„hoch“ eingereicht werden, den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus sollten die nationalen Behörden für die Cybersicherheitszertifizierung mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen mit den Anforderungen dieser Verordnung oder bestimmten europäischen Schemata für die Cybersicherheitszertifizierung austauschen. Die Kommission sollte diesen Informationsaustausch erleichtern, indem sie ein allgemeines elektronisches Informationssystem zur Unterstützung bereitstellt, zum Beispiel das internetgestützte Informations- und Kommunikationssystem zur europaweiten Marktüberwachung (Information and Communication System on Market Surveillance — ICSMS) und das gemeinschaftliche System zum raschen Austausch von Informationen über die Gefahren bei der Verwendung von Konsumgütern (Community system for the rapid exchange of information on dangers arising from the use of consumer products — RAPEX), die in Übereinstimmung mit der Verordnung (EG) Nr. 765/2008 bereits von Marktüberwachungsbehörden genutzt werden.

(103) Für eine einheitliche Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung sollte eine europäische Gruppe für die Cybersicherheitszertifizierung eingesetzt werden, die sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder anderer zuständiger nationaler Behörden zusammensetzt. Die Gruppe für die Cybersicherheitszertifizierung sollte vor allem die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung beraten und unterstützen, die ENISA bei der Ausarbeitung der möglichen Cybersicherheitszertifizierungsschemata unterstützen und mit ihr eng zusammenarbeiten, in entsprechend begründeten Fällen die ENISA mit der Ausarbeitung eines möglichen Schemas beauftragen, an die ENISA gerichtete Stellungnahmen zu möglichen Schemata annehmen, und an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Schemata für die Cybersicherheitszertifizierung annehmen. Die Gruppe für die Cybersicherheitszertifizierung sollte den Austausch von bewährten Verfahren und Sachkenntnissen zwischen den verschiedenen nationalen Behörden für die Cybersicherheitszertifizierung, die für die Ermächtigung der Konformitätsbewertungsstellen und die Ausstellung von Europäischen Cybersicherheitszertifikaten zuständig sind, erleichtern.

(104) Zur Sensibilisierung und um die Akzeptanz künftiger europäischer Schemata für die Cybersicherheitssicherheit zu erhöhen, kann die Kommission allgemeine und sektorspezifische Cybersicherheitsleitlinien herausgeben, die sich beispielsweise auf bewährte Verfahren oder verantwortungsvolles Verhalten im Bereich der Cybersicherheit beziehen, und dabei die Vorteile der Verwendung zertifizierter IKT-Produkte, -Dienste und -Prozesse hervorheben.

(105) Da die IKT-Lieferketten weltumspannend sind, kann die Union zur weiteren Erleichterung des Handels gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Abkommen über die gegenseitige Anerkennung von europäischen Cybersicherheitszertifikaten schließen. Die Kommission kann unter Berücksichtigung der Ratschläge der ENISA und der europäischen Gruppe für die Cybersicherheitszertifizierung die Aufnahme entsprechender Verhandlungen empfehlen. In jedem europäischen Schema für die Cybersicherheitszertifizierung sollten spezifische Bedingungen für diese Abkommen über die gegenseitige Anerkennung bei Drittländern vorgesehen werden.

(106) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([22]) ausgeübt werden.

(107) Das Prüfverfahren sollte für die Annahme der Durchführungsrechtsakte über die europäischen Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten oder -Prozessen, für die Annahme von Durchführungsrechtsakten über die Modalitäten für die Durchführung von Umfragen durch die ENISA, für die Annahme von Durchführungsrechtsakten über einen Plan für die gegenseitige Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung sowie für die Annahme von Durchführungsrechtsakten über die Umstände, Formate und Verfahren der Notifikation akkreditierter Konformitätsbewertungsstellen durch die nationalen Behörden für die Cybersicherheitszertifizierung bei der Kommission verwendet werden.

(108) Die Tätigkeit der ENISA sollte regelmäßig und unabhängig bewertet werden. Diese Bewertung sollte sich darauf beziehen, inwieweit die ENISA ihre Ziele erreicht, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind, insbesondere ihre Aufgaben bezüglich der operativen Zusammenarbeit auf Unionsebene. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden. Im Falle einer Überprüfung sollte die Kommission bewerten, wie die Rolle der ENISA als Bezugspunkt für Beratung und Sachkenntnis verstärkt werden kann und sollte ebenfalls die Möglichkeit einer Rolle der ENISA bei der Unterstützung der Bewertung von IKT-Produkten, -Diensten und -Prozessen aus Drittländern, die auf den Unionsmarkt gelangen und gegen die Unionsvorschriften verstoßen, bewerten.

([22]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

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

(110) Die Verordnung (EU) Nr. 526/2013 sollte aufgehoben werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

TITEL I

ALLGEMEINE BESTIMMUNGEN

Artikel 1

Gegenstand und Geltungsbereich

(1) Um das ordnungsgemäße Funktionieren des Binnenmarkts zu gewährleisten und um gleichzeitig in der Union ein hohes Niveau in der Cybersicherheit, bei der Fähigkeit zur Abwehr gegen Cyberangriffe und beim Vertrauen in die Cybersicherheit zu erreichen, wird in dieser Verordnung Folgendes festgelegt:

a) die Ziele, Aufgaben und organisatorischen Aspekte der ENISA (Agentur der Europäischen Union für Cybersicherheit) und

b) ein Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung, mit dem Ziel, für IKT-Produkte und -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und mit dem Ziel, eine Fragmentierung des Binnenmarkts bei Zertifizierungsschemata, in der Union zu verhindern.

Der Rahmen nach Unterabsatz 1 Buchstabe b gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

(2) Von dieser Verordnung unberührt bleiben die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

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

2. „Netz- und Informationssystem“ bezeichnet ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie (EU) 2016/1148;

3. „nationale Strategie für die Sicherheit von Netz- und Informationssystemen“ bezeichnet eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 4 Nummer 3 der Richtlinie (EU) 2016/1148;

4. „Betreiber wesentlicher Dienste“ bezeichnet einen Betreiber wesentlicher Dienste im Sinne des Artikels 4 Nummer 4 der Richtlinie (EU) 2016/1148;

5. „Anbieter digitaler Dienste“ bezeichnet einen Anbieter digitaler Dienste im Sinne des Artikels 4 Nummer 6 der Richtlinie (EU) 2016/1148;

6. „Sicherheitsvorfall“ bezeichnet einen Sicherheitsvorfall im Sinne des Artikels 4 Nummer 7 der Richtlinie (EU) 2016/1148;

7. „Bewältigung von Sicherheitsvorfällen“ bezeichnet die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 4 Nummer 8 der Richtlinie (EU) 2016/1148;

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

9. „europäisches Schema für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, -Diensten und -Prozessen gelten;

10. „nationales Schema für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die für die Zertifizierung oder Konformitätsbewertung von IKT-Produkten, -Diensten und -Prozessen gelten, die von diesem Schema erfasst werden;

11. „europäisches Cybersicherheitszertifikat“ bezeichnet ein von der maßgeblichen Stelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst oder ein bestimmter IKT-Prozess im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde;

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

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

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

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

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

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

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

19. „Norm“ bezeichnet eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012;

20. „technische Spezifikation“ bezeichnet ein Dokument, in dem die technischen Anforderungen, denen ein IKT-Prozess, -Produkt oder -Dienst genügen muss oder ein diesbezügliches Konformitätsbewertungsverfahren vorgeschrieben sind;

21. „Vertrauenswürdigkeitsstufe“ bezeichnet die Grundlage für das Vertrauen darin, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines spezifischen europäischen Schemas für die Cybersicherheitszertifizierung genügt, gibt an, auf welchem Niveau das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess, bei der Bewertung eingestuft wurde, misst jedoch als solche nicht die Sicherheit des IKT-Produkts, -Dienstes oder -Prozesses;

22. „Selbstbewertung der Konformität“ bezeichnet eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Bewertung, ob diese IKT- Produkte, -Dienste oder -Prozesse die Anforderungen, die in einem spezifischen europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, erfüllen.

TITEL II

ENISA (AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT)

KAPITEL I

Mandat und Ziele

Artikel 3

Mandat

(1) Die ENISA nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union zu erreichen, unter anderem indem sie die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Verbesserung der Cybersicherheit unterstützt. Die ENISA dient den Organen, Einrichtungen und sonstigen Stellen der Union sowie anderen maßgeblichen Interessenträgern der Union als Bezugspunkt für Beratung und Sachkenntnis im Bereich Cybersicherheit.

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

(2) Die ENISA nimmt die ihr durch Rechtsakte der Union zugewiesenen Aufgaben wahr, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der Cybersicherheit angeglichen werden sollen.

(3) Die ENISA handelt bei der Wahrnehmung ihrer Aufgaben unabhängig, vermeidet Überschneidungen mit den Tätigkeiten der Mitgliedstaaten und berücksichtigt die bereits vorhandene Sachkenntnis der Mitgliedstaaten.

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

Artikel 4

Ziele

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

(2) Die ENISA unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Ausarbeitung und Umsetzung von Strategien der Union im Zusammenhang mit der Cybersicherheit, wozu auch sektorbezogene Strategien zur Cybersicherheit gehören.

(3) Die ENISA fördert unionsweit den Kapazitätsaufbau und die Abwehrbereitschaft, indem sie die Organe, Einrichtungen und sonstigen Stellen der Union, die Mitgliedstaaten sowie öffentliche und private Interessenträger dabei unterstützt, den Schutz ihrer Netz- und Informationssysteme zu verbessern, Fähigkeiten zur Abwehr von Cyberangriffen und Reaktionskapazitäten aufzubauen und zu verbessern und Fähigkeiten und Kompetenzen auf dem Gebiet der Cybersicherheit aufzubauen.

(4) Die ENISA fördert auf Unionsebene die Zusammenarbeit einschließlich des Informationsaustauschs und die Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen privaten und öffentlichen Interessenträgern in Fragen, die im Zusammenhang mit der Cybersicherheit stehen.

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

(6) Die ENISA fördert die Nutzung der europäischen Cybersicherheits-Zertifizierung, um der Fragmentierung des Binnenmarkts vorzubeugen. Die ENISA trägt zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens im Sinne des Titels III dieser Verordnung bei, um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt sowie dessen Wettbewerbsfähigkeit zu stärken.

(7) Die ENISA fördert ein hohes Maß der Sensibilisierung für die Cybersicherheit, einschließlich der Cyberhygiene und der Cyberkompetenz von Bürgern, Organisationen und Unternehmen.

KAPITEL II

Aufgaben

Artikel 5

Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts

Die ENISA trägt zur Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts bei, indem sie

1. insbesondere durch unabhängige Stellungnahmen und Analysen sowie durch vorbereitende Arbeiten zur Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit Beratung und Unterstützung gewährt und indem sie sektorspezifische Strategien und Rechtsetzungsinitiativen im Bereich der Cybersicherheit vorlegt;

2. die Mitgliedstaaten darin unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit, vor allem im Zusammenhang mit der Richtlinie (EU) 2016/1148, kohärent umzusetzen, auch durch die Abgabe von Stellungnahmen, Herausgabe von Leitlinien, Anbieten von Beratung und bewährten Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsaustausch, und indem sie den Austausch bewährter Verfahren in diesem Bereich zwischen den zuständigen Behörden erleichtert;

3. die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Entwicklung und Förderung von Strategien im Zusammenhang mit der Cybersicherheit unterstützt, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des offenen Internets bewahren;

4. ihre Sachkenntnis und Unterstützung in die Arbeit der nach Artikel 11 der Richtlinie (EU) 2016/1148 eingesetzten Kooperationsgruppe einbringt;

5. Folgendes unterstützt:

   a) die Entwicklung und Umsetzung der Unionspolitik im Bereich der elektronischen Identität und Vertrauensdienste, vor allem durch Beratung und die Herausgabe technische Leitlinien sowie durch die Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden;

   b) die Förderung eines höheren Sicherheitsniveaus in der elektronischen Kommunikation, auch indem sie Beratung und Sachkenntnis anbietet und den Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtert;

   c) die Mitgliedstaaten bei der Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre, was — auf dessen Ersuchen die Beratung des Europäischen Datenschutzausschusses einschließt;

6. die regelmäßige Überprüfung der Unionspolitik unterstützt und dazu einen Jahresbericht über den Stand der Umsetzung des jeweiligen Rechtsrahmens in Bezug auf Folgendes erstellt:

   a) Informationen über Meldungen von Sicherheitsvorfällen durch die Mitgliedstaaten über die zentrale Anlaufstelle der Kooperationsgruppe nach Artikel 10 Absatz 3 der Richtlinie (EU) 2016/1148;

   b) Zusammenfassungen von Meldungen von Sicherheitsverletzungen oder Integritätsverlusten von Vertrauensdiensteanbietern, die der ENISA auf der Grundlage des Artikels 19 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([23]) von den Aufsichtsstellen übermittelt werden;

   c) die Meldungen von Sicherheitsvorfällen durch Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste, die der ENISA von den zuständigen Behörden auf der Grundlage des Artikels 40 der Richtlinie (EU) 2018/1972 übermittelt werden.

([23]) Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt) gefördert werden und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

Artikel 6

Kapazitätsaufbau

(1) Die ENISA unterstützt

a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Fähigkeiten bei der Bewältigung von Cyberbedrohungen und Cybersicherheitsvorfällen, indem sie ihnen Wissen und Sachkenntnisse zur Verfügung stellt;

b) die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Aufstellung und Umsetzung von Strategien für eine Offenlegung von Sicherheitslücken auf freiwilliger Basis;

c) die Organe, Einrichtungen und sonstigen Stellen der Union bei ihren Bemühungen zur Verhütung, Erkennung und Analyse von Cyberbedrohungen und Cybersicherheitsvorfällen und zur Verbesserung ihrer Fähigkeiten bei der Bewältigung derartiger Cyberbedrohungen und Cybersicherheitsvorfällen, indem sie insbesondere das CERT-EU angemessen unterstützt;

d) die Mitgliedstaaten auf deren Ersuchen beim Aufbau nationaler CSIRTs nach Artikel 9 Absatz 5 der Richtlinie (EU) 2016/1148;

e) die Mitgliedstaaten auf Ersuchen bei der Ausarbeitung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen nach Artikel 7 Absatz 2 der Richtlinie (EU) 2016/1148 und fördert die unionsweite Verbreitung dieser Strategien und stellt die Fortschritte bei deren Umsetzung fest, um bewährte Verfahren bekannt zu machen;

f) die Organe der Union bei der Ausarbeitung und Überprüfung von Unionsstrategien zur Cybersicherheit, fördert deren Verbreitung und verfolgt die Fortschritte bei deren Umsetzung;

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

h) die Mitgliedstaaten durch die regelmäßige Veranstaltung der mindestens alle zwei Jahre stattfindenden Cybersicherheitsübungen auf Unionsebene nach Artikel 7 Absatz 5 und durch die Abgabe von Empfehlungen, die sie aus der Auswertung der Übungen und der bei diesen gemachten Erfahrungen ableitet;

i) einschlägige öffentliche Stellen, indem sie diesen, gegebenenfalls in Zusammenarbeit mit Interessenträgern, Fortbildungen zur Cybersicherheit anbietet;

j) die Kooperationsgruppe beim Austausch bewährter Verfahren, vor allem zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten nach Artikel 11 Absatz 3 Buchstabe l der Richtlinie (EU) 2016/1148, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten, im Hinblick auf Risiken und Sicherheitsvorfälle.

(2) Die ENISA unterstützt den Informationsaustausch in und zwischen den Sektoren, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren sowie zur Bewältigung rechtlicher Fragen im Zusammenhang mit dem Informationsaustausch bereitstellt.

Artikel 7

Operative Zusammenarbeit auf Unionsebene

(1) Die ENISA unterstützt die operative Zusammenarbeit zwischen den Mitgliedstaaten und Organen, Einrichtungen und sonstigen Stellen der Union untereinander und zwischen den Interessenträgern.

(2) Die ENISA arbeitet auf operativer Ebene mit den Organen, Einrichtungen und sonstigen Stellen der Union zusammen und entwickelt Synergien mit diesen Stellen, zu denen auch das CERT-EU sowie die für Cyberkriminalität und die Aufsicht über den Datenschutz zuständigen Stellen zählen, um Fragen von gemeinsamem Interesse anzugehen, unter anderem durch

a) den Austausch von Know-how und bewährten Verfahren;

b) die Bereitstellung von Beratung und die Veröffentlichung von Leitlinien zu einschlägigen Fragen im Zusammenhang mit der Cybersicherheit;

c) die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben nach Konsultation der Kommission.

(3) Die ENISA führt die Sekretariatsgeschäfte des CSIRTs-Netzes nach Artikel 12 Absatz 2 der Richtlinie (EU) 2016/1148 und unterstützt in dieser Eigenschaft aktiv den Informationsaustausch und die Zusammenarbeit zwischen den Mitgliedern des CSIRTs-Netzes.

(4) Die ENISA unterstützt die Mitgliedstaaten bei der operativen Zusammenarbeit innerhalb des CSIRTs-Netzes, indem sie

a) diese berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können, und auf Ersuchen eines oder mehrerer Mitgliedstaaten Beratung in Bezug auf eine spezifische Cyberbedrohung leistet;

b) auf Ersuchen eines oder mehrerer Mitgliedstaaten bei der Bewertung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen Hilfe leistet, indem sie Sachkenntnisse bereitstellt und die technische Bewältigung solcher Vorfälle erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe maßgeblicher Informationen und technischer Lösungen zwischen den Mitgliedstaaten;

c) Sicherheitslücken und Sicherheitsvorfälle auf der Grundlage von öffentlich verfügbaren Informationen oder freiwillig von den Mitgliedstaaten zu diesem Zweck bereitgestellten Informationen analysiert und

d) auf Ersuchen eines oder mehrerer Mitgliedstaaten die nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen im Sinne der Richtlinie (EU) 2016/1148 unterstützt.

Bei der Wahrnehmung dieser Aufgaben arbeiten die ENISA und das CERT-EU in strukturierter Weise zusammen, um Synergien nutzen zu können und Doppelarbeit zu vermeiden.

(5) Die ENISA veranstaltet auf Unionsebene regelmäßig Cybersicherheitsübungen und unterstützt die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union auf deren Ersuchen hin bei der Organisation solcher Cybersicherheitsübungen. Diese Cybersicherheitsübungen auf Unionsebene können technische, operative oder strategische Elemente umfassen. Alle zwei Jahre veranstaltet die ENISA eine umfassende Großübung.

Die ENISA unterstützt gemeinsam mit den betreffenden Organisationen gegebenenfalls auch die Organisation sektorspezifischer Cybersicherheitsübungen, zu denen sie beiträgt, wobei diese Organisationen an den Cybersicherheitsübungen auf Unionsebene teilnehmen können.

(6) Die ENISA erstellt in enger Zusammenarbeit mit den Mitgliedstaaten regelmäßig einen eingehenden technischen EU-Cybersicherheitslagebericht über Sicherheitsvorfälle und Bedrohungen auf der Grundlage von öffentlich zugänglichen Informationen, eigenen Analysen und Berichten, die ihr unter anderem von den CSIRTs der Mitgliedstaaten () oder den zentralen Anlaufstellen im Sinne der Richtlinie (EU) 2016/1148 (in beiden Fällen auf freiwilliger Basis) sowie dem EC3 und dem CERT-EU übermittelt werden.

(7) Die ENISA trägt zur Entwicklung gemeinsamer Maßnahmen bei, mit denen auf Ebene der Union und der Mitgliedstaaten auf massive, grenzüberschreitende Cybersicherheitsvorfälle oder Cyberkrisen reagiert werden kann, indem sie insbesondere:

a) öffentlich verfügbare oder auf freiwilliger Grundlage bereitgestellte Berichte aus nationalen Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt und analysiert;

b) für einen effizienten Informationsfluss und Mechanismen sorgt, die zwischen dem CSIRTs-Netz und den fachlichen und politischen Entscheidungsträgern auf EU-Ebene eine abgestufte Vorgehensweise ermöglichen;

c) auf Ersuchen die technische Bewältigung dieser Sicherheitsvorfälle oder Krisen erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe technischer Lösungen zwischen den Mitgliedstaaten;

d) die Organe, Einrichtungen und sonstigen Stellen der Union und auf deren Ersuchen die Mitgliedstaaten bei der öffentlichen Kommunikation im Umfeld solcher Sicherheitsvorfälle oder der Krisen unterstützt;

e) die Kooperationspläne für die Reaktion auf solche Sicherheitsvorfälle oder Krisen auf Ebene der Union testet und auf deren Ersuchen die Mitgliedstaaten bei der Erprobung solcher Pläne auf nationaler Ebene unterstützt.

Artikel 8

Markt, Cybersicherheitszertifizierung und Normung

(1) Die ENISA unterstützt und fördert die Entwicklung und Umsetzung der Unionspolitik auf dem Gebiet der Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, wie in Titel III dieser Verordnung festgelegt, indem sie

a) die Entwicklungen in damit zusammenhängenden Normungsbereichen fortlaufend überwacht und in Fällen, in denen keine Normen zur Verfügung stehen, geeignete technische Spezifikationen für die Entwicklung europäischer Schemata für die Cybersicherheitszertifizierung nach Artikel 54 Absatz 1 Buchstabe c empfiehlt;

b) mögliche europäische Schemata für die Cybersicherheitszertifizierung (im Folgenden „mögliche Schemata“) von IKT-Produkten, -Diensten und -Prozessen nach Artikel 49 ausarbeitet;

c) angenommene europäische Schemata für die Cybersicherheitszertifizierung nach Artikel 49 Absatz 8 evaluiert;

d) sich an gegenseitigen Begutachtungen nach Artikel 59 Absatz 4 beteiligt;

e) die Kommission bei der Wahrnehmung der Sekretariatsgeschäfte der nach Artikel 62 Absatz 5 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung unterstützt.

(2) Die ENISA nimmt die Sekretariatsgeschäfte der nach Artikel 22 Absatz 4 eingesetzten Gruppe der Interessenträger für die Cybersicherheitszertifizierung wahr.

(3) Die ENISA stellt in Zusammenarbeit mit den nationalen Behörden für die Cybersicherheitszertifizierung und der Branche auf formelle, strukturierte und transparente Art und Weise Leitlinien zusammen und veröffentlicht diese und entwickelt bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen.

(4) Die ENISA trägt zu einem hinreichenden Kapazitätsaufbau im Zusammenhang mit den Bewertungs- und Zertifizierungsverfahren bei, indem sie Leitlinien erstellt und veröffentlicht und die Mitgliedstaaten auf deren Ersuchen hin unterstützt.

(5) Die ENISA erleichtert die Ausarbeitung und Übernahme europäischer und internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten, -Diensten und -Prozessen.

(6) Die ENISA bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten und der Branche Beratung an und erstellt Leitlinien für die technischen Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten.

(7) Die ENISA führt regelmäßig Analysen der wichtigsten Angebots- und Nachfragetrends auf dem Cybersicherheitsmarkt durch, um den Cybersicherheitsmarkt in der Union zu fördern.

Artikel 9

Wissen und Informationen

Die ENISA

a) führt Analysen neu entstehender Technik durch und bietet themenspezifische Bewertungen der von den technischen Innovationen zu erwartenden gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Auswirkungen auf die Cybersicherheit;

b) führt langfristige strategische Analysen der Cyberbedrohungen und Sicherheitsvorfälle durch, um neu auftretende Trends erkennen und dazu beitragen zu können, Sicherheitsvorfälle zu vermeiden;

c) stellt in Zusammenarbeit mit den Sachverständigen der Behörden der Mitgliedstaaten und den maßgeblichen Interessenträgern Beratung, Leitlinien und bewährte Verfahren für die Sicherheit der Netz- und Informationssysteme zur Verfügung, vor allem für die Sicherheit der Infrastrukturen, die die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren unterstützen, und der Infrastrukturen, die von den Anbietern der in Anhang III der genannten Richtlinie aufgeführten digitaler Dienste genutzt werden;

d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit und die auf freiwilliger Grundlage von den Mitgliedstaaten und privaten und öffentlichen Interessenträgern bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

e) erhebt und analysiert öffentlich verfügbare Informationen über signifikante Sicherheitsvorfälle und stellt Berichte mit dem Ziel zusammen, den Bürgern, Organisationen und Unternehmen unionsweite Leitlinien bereitzustellen.

Artikel 10

Sensibilisierung und Ausbildung

Die ENISA

a) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren für einzelne Nutzer zur Verfügung, die sich an Bürger, Organisationen und Unternehmen richten und auch Cyberhygiene und Cyberkompetenz umfassen;

b) organisiert in Zusammenarbeit mit den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und der Branche regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen und eine umfassende öffentliche Debatte anzuregen;

c) unterstützt die Mitgliedstaaten bei ihren Anstrengungen zur Sensibilisierung in Bezug auf Cybersicherheit und zur Förderung der Ausbildung im Bereich Cybersicherheit;

d) unterstützt die engere Koordinierung und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten in Bezug auf Sensibilisierung und Ausbildung im Bereich Cybersicherheit.

Artikel 11

Forschung und Innovation

Die ENISA, in Zusammenhang mit der Forschung und Innovation,

a) berät die Organe, Einrichtungen und sonstigen Stellen der Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Cyberbedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnologien (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

b) beteiligt sich dort, wo die Kommission ihr die einschlägigen Befugnisse übertragen hat, an der Durchführungsphase von Förderprogrammen für Forschung und Innovation oder als Begünstige;

c) trägt im Bereich der Cybersicherheit zur strategischen Forschungs- und Innovationsagenda auf Unionsebene bei.

Artikel 12

Internationale Zusammenarbeit

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

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

b) auf Ersuchen der Kommission den Austausch bewährter Verfahren erleichtert;

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

d) die Kommission in Zusammenarbeit mit der nach Artikel 62 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung bei Fragen zu Abkommen über die gegenseitige Anerkennung von Cybersicherheitszertifikaten mit Drittländern berät und unterstützt.

KAPITEL III

Organisation der ENISA

Artikel 13

Struktur der ENISA

Die Verwaltungs- und Leitungsstruktur der ENISA besteht aus

a) einem Verwaltungsrat;

b) einem Exekutivrat;

c) einem Exekutivdirektor;

d) einer EINSA-Beratungsgruppe; und

e) einem Netz der nationalen Verbindungsbeamten.

Abschnitt 1

Verwaltungsrat

Artikel 14

Zusammensetzung des Verwaltungsrats

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

(2) Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter. Dieser Stellvertreter vertritt das Mitglied im Fall seiner Abwesenheit.

(3) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter werden aufgrund ihrer Kenntnisse auf dem Gebiet der Cybersicherheit ernannt, wobei ihren einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen Rechnung zu tragen ist. Die Kommission und die Mitgliedstaaten bemühen sich, die Fluktuation bei ihren Vertretern im Verwaltungsrat gering zu halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen. Die Kommission und die Mitgliedstaaten setzen sich für ein ausgewogenes Geschlechterverhältnis im Verwaltungsrat ein.

(4) Die Amtszeit der Mitglieder des Verwaltungsrats und ihrer Stellvertreter beträgt vier Jahre. Sie kann verlängert werden.

Artikel 15

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat

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

b) nimmt den Entwurf des in Artikel 24 genannten einheitlichen Programmplanungsdokuments der ENISA an, bevor dieser der Kommission zur Stellungnahme vorgelegt wird;

c) nimmt — unter Berücksichtigung der Stellungnahme der Kommission — das einheitliche Programmplanungsdokument der ENISA an;

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

e) stellt den jährlichen Haushaltsplan der Agentur fest und übt andere Funktionen in Bezug auf den Haushalt der ENISA gemäß Kapitel IV aus;

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

g) erlässt nach Artikel 32 die für die ENISA geltende Finanzregelung;

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

i) erlässt Vorschriften zur Unterbindung und Bewältigung von Interessenkonflikten bei seinen Mitgliedern;

j) sorgt ausgehend von den Erkenntnissen und Empfehlungen, die sich aus den Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und den verschiedenen internen und externen Prüfberichten und Bewertungen ergeben haben, für angemessene Folgemaßnahmen;

k) gibt sich eine Geschäftsordnung einschließlich Regelungen zu den vorläufigen Beschlüssen zur Übertragung bestimmter Aufgaben gemäß Artikel 19 Absatz 7;

l) nimmt gemäß Absatz 2 des vorliegenden Artikels in Bezug auf das Personal der ENISA die Befugnisse wahr, die der Anstellungsbehörde durch das Statut der Beamten der Europäischen Union (im Folgenden „Statut der Beamten") bzw. der Stelle, die zum Abschluss der Dienstverträge ermächtigt ist, durch die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union (im Folgenden „Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union") nach der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([24]) übertragen wurden (im Folgenden „Befugnisse der Anstellungsbehörde");

m) erlässt gemäß dem Verfahren des Artikels 110 des Statuts der Beamten Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen für die sonstigen Bediensteten;

n) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 36 seines Amtes;

o) ernennt einen Rechnungsführer, bei dem es sich um den Rechnungsführer der Kommission handeln kann, der in der Wahrnehmung seiner Aufgaben völlig unabhängig ist;

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

q) genehmigt das Treffen von Arbeitsvereinbarungen bezüglich Artikel 7;

r) genehmigt das Treffen oder den Abschluss von Arbeitsvereinbarungen nach Artikel 42.

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

([24]) Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1).

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

Artikel 16

Vorsitz des Verwaltungsrats

Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder mit der Zweidrittelmehrheit seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden. Ihre Amtszeit beträgt vier Jahre, wobei eine einmalige Wiederwahl zulässig ist. Endet jedoch ihre Mitgliedschaft im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch am selben Tag. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle.

Artikel 17

Sitzungen des Verwaltungsrats

(1) Der Verwaltungsrat wird von seinem Vorsitzenden einberufen.

(2) Der Verwaltungsrat tritt mindestens zweimal jährlich zu einer ordentlichen Sitzung zusammen. Auf Antrag des Vorsitzenden, der Kommission oder mindestens eines Drittels seiner Mitglieder tritt er darüber hinaus zu außerordentlichen Sitzungen zusammen.

(3) Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats teil, hat jedoch kein Stimmrecht.

(4) Die Mitglieder der ENISA-Beratungsgruppe können auf Einladung des Vorsitzes an den Sitzungen des Verwaltungsrats teilnehmen, haben jedoch kein Stimmrecht.

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

(6) Die Sekretariatsgeschäfte des Verwaltungsrats werden von der ENISA wahrgenommen.

Artikel 18

Vorschriften für die Abstimmung im Verwaltungsrat

(1) Der Verwaltungsrat fasst seine Beschlüsse mit der Mehrheit seiner Mitglieder.

(2) Für die Annahme des einheitlichen Programmplanungsdokuments und des jährlichen Haushaltsplans sowie für die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors ist eine Mehrheit von zwei Dritteln der Mitglieder des Verwaltungsrats erforderlich.

(3) Jedes Mitglied hat eine Stimme. In Abwesenheit eines Mitglieds kann sein Stellvertreter das Stimmrecht des Mitglieds ausüben.

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

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

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

Abschnitt 2

Exekutivrat

Artikel 19

Exekutivrat

(1) Der Verwaltungsrat wird von einem Exekutivrat unterstützt.

(2) Der Exekutivrat

a) bereitet die Beschlussvorlagen für den Verwaltungsrat vor;

b) stellt zusammen mit dem Verwaltungsrat sicher, dass ausgehend von den Ergebnissen und Empfehlungen im Rahmen der Untersuchungen des OLAF und der externen oder internen Prüfberichte und Bewertungen angemessene Folgemaßnahmen getroffen werden;

c) unterstützt und berät unbeschadet der Aufgaben des Exekutivdirektors nach Artikel 20 den Exekutivdirektor bei der Umsetzung der verwaltungs- und haushaltsbezogenen Beschlüsse des Verwaltungsrats nach Artikel 20.

(3) Der Exekutivrat besteht aus fünf Mitgliedern. Die Mitglieder des Exekutivrats werden aus den Reihen der Mitglieder des Verwaltungsrats ernannt. Eines der Mitglieder ist der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und ein weiteres ist einer der Vertreter der Kommission. Bei den Ernennungen der Mitglieder des Exekutivrats wird die Sicherstellung eines ausgewogenen Geschlechterverhältnisses im Exekutivrat angestrebt. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats, hat jedoch kein Stimmrecht.

(4) Die Amtszeit der Mitglieder des Exekutivrats beträgt vier Jahre. Sie kann verlängert werden.

(5) Der Exekutivrat tritt mindestens einmal alle drei Monate zusammen. Der Vorsitzende des Exekutivrats beruft auf Antrag der Mitglieder zusätzliche Sitzungen ein.

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

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

Abschnitt 3

Exekutivdirektor

Artikel 20

Pflichten des Exekutivdirektors

(1) Die ENISA wird von ihrem Exekutivdirektor geleitet, der bei der Wahrnehmung seiner Aufgaben unabhängig ist. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig.

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

(3) Der Exekutivdirektor ist dafür verantwortlich,

a) die laufenden Geschäfte der ENISA zu führen;

b) die vom Verwaltungsrat gefassten Beschlüsse umzusetzen;

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

d) das einheitliche Programmplanungsdokument umzusetzen und dem Verwaltungsrat hierüber Bericht zu erstatten;

e) den konsolidierten Jahresbericht über die Tätigkeit der ENISA, einschließlich der Umsetzung des jährlichen Arbeitsprogramms der ENISA, auszuarbeiten und dem Verwaltungsrat zur Bewertung und Annahme vorzulegen;

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

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

h) den Entwurf der für die ENISA geltenden Finanzregelung nach Artikel 32 auszuarbeiten;

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

j) die finanziellen Interessen der Union durch vorbeugende Maßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und, falls Unregelmäßigkeiten festgestellt werden, durch Einziehung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch Verhängung wirksamer, verhältnismäßiger und abschreckender verwaltungsrechtlicher und finanzieller Sanktionen zu schützen;

k) eine Betrugsbekämpfungsstrategie für die ENISA auszuarbeiten und dem Verwaltungsrat zur Genehmigung vorzulegen;

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

m) einen regelmäßigen Gedanken- und Informationsaustausch mit den Organen, Einrichtungen und sonstigen Stellen der Union über deren Tätigkeiten im Bereich Cybersicherheit zu führen, um die Kohärenz bei der Weiterentwicklung und Umsetzung der Unionspolitik sicherzustellen;

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

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

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

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

Abschnitt 4

ENISA-Beratungsgruppe, Gruppe der Interessenträger für die Cybersicherheitszertifizierung und Netz der nationalen Verbindungsbeamten

Artikel 21

ENISA-Beratungsgruppe

(1) Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors auf transparente Art und Weise eine ENISA-Beratungsgruppe ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, KMU, Betreiber wesentlicher Dienste, Verbrauchergruppen, wissenschaftliche Sachverständige aus dem Bereich der Cybersicherheit sowie Vertreter der zuständigen Behörden, die nach der Richtlinie (EU) 2018/1972 notifiziert wurden, europäische Normungsorganisationen sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden. Der Verwaltungsrat strebt ein angemessenes Gleichgewicht zwischen den Geschlechtern, ein angemessenes geographisches Gleichgewicht und ein angemessenes Gleichgewicht zwischen den verschiedenen Interessengruppen an.

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

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

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

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

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

Artikel 22

Gruppe der Interessenträger für die Cybersicherheitszertifizierung

(1) Es wird eine Gruppe der Interessenträger für die Cybersicherheitszertifizierung eingesetzt.

(2) Die Mitglieder der Gruppe der Interessenträger für die Cybersicherheitszertifizierung werden unter anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger ausgewählt. Die Kommission wählt die Mitglieder der Gruppe der Interessenträger für die Cybersicherheitszertifizierung auf Vorschlag der ENISA im Wege eines transparenten und offenen Auswahlverfahrens aus, durch das ein Gleichgewicht zwischen den verschiedenen Interessengruppen sowie ein angemessenes Gleichgewicht zwischen den Geschlechtern und ein angemessenes geographisches Gleichgewicht sichergestellt wird.

(3) Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung:

a) berät die Kommission in strategischen Fragen im Zusammenhang mit dem europäischen Rahmen für die Cybersicherheitszertifizierung;

b) berät auf Ersuchen die ENISA in allgemeinen und strategischen Fragen im Zusammenhang mit den Aufgaben der ENISA in Bezug auf den Markt, die Cybersicherheitszertifizierung und die Normung;

c) unterstützt die Kommission bei der Ausarbeitung des in Artikel 47 genannten fortlaufenden Arbeitsprogramms der Union;

d) nimmt zum fortlaufenden Arbeitsprogramm der Union gemäß Artikel 47 Absatz 4 Stellung und

e) berät in dringenden Fällen die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung in Bezug auf die Notwendigkeit zusätzlicher Zertifizierungsschemata, die nicht Teil des fortlaufenden Arbeitsprogramms der Union sind, wie in Artikel 47 und 48 beschrieben.

(4) Den Vorsitz der Gruppe der Interessenträger für die Cybersicherheitszertifizierung führen die Vertreter der Kommission und der ENISA gemeinsam, und die Sekretariatsgeschäfte werden von der ENISA wahrgenommen.

Artikel 23

Netz der nationalen Verbindungsbeamten

(1) Der Verwaltungsrat richtet auf Vorschlag des Exekutivdirektors ein Netz der nationalen Verbindungsbeamten ein, das sich aus Vertretern der Mitgliedstaaten zusammensetzt (im Folgenden „nationale Verbindungsbeamten"). Jeder Mitgliedstaat ernennt einen Vertreter im Netz der nationalen Verbindungsbeamten. Die Sitzungen des Netzes der nationalen Verbindungsbeamten können in verschiedenen Sachverständigenzusammensetzungen abgehalten werden.

(2) Das Netz der nationalen Verbindungsbeamten erleichtert vor allem den Informationsaustausch zwischen der ENISA und den Mitgliedstaaten und unterstützt die ENISA dabei, ihre Tätigkeiten, Erkenntnisse und Empfehlungen bei den einschlägigen Interessenträgern in der gesamten Union bekannt zu machen.

(3) Die nationalen Verbindungsbeamten dienen als Kontaktstelle auf nationaler Ebene, um die Zusammenarbeit zwischen der ENISA und den nationalen Sachverständigen im Rahmen der Durchführung des Jahresarbeitsprogramms der ENISA zu erleichtern.

(4) Während die nationalen Verbindungsbeamten eng mit den Vertretern ihres jeweiligen Mitgliedstaats im Verwaltungsrat zusammenarbeiten, darf das Netz der nationalen Verbindungsbeamten selbst nicht dieselbe Arbeit leisten wie der Verwaltungsrat oder andere Gremien der Union.

(5) Die Funktionen und Verfahren des Netzes der nationalen Verbindungsbeamten werden in den internen Verfahrensvorschriften der ENISA festgelegt und der Öffentlichkeit zugänglich gemacht.

Abschnitt 5

Arbeitsweise

Artikel 24

Einheitliches Programmplanungsdokument

(1) Die ENISA führt ihre Geschäfte in Übereinstimmung mit einem einheitlichen Programmplanungsdokument, das ihre jährliche und mehrjährige Programmplanung mit allen ihren geplanten Tätigkeiten enthält.

(2) Jedes Jahr erstellt der Exekutivdirektor einen Entwurf des einheitlichen Programmplanungsdokuments mit der jährlichen und mehrjährigen Programmplanung und der entsprechenden Finanz- und Personalplanung nach Artikel 32 der Delegierten Verordnung (EU) Nr. 1271/2013 der Kommission ([25]) und unter Berücksichtigung der von der Kommission festgelegten Leitlinien.

(3) Bis zum 30. November eines jeden Jahres nimmt der Verwaltungsrat das in Absatz 1 genannte einheitliche Programmplanungsdokument an und übermittelt es bis zum 31. Januar des Folgejahres dem Europäischen Parlament, dem Rat und der Kommission, sowie jede spätere Aktualisierung dieses Dokuments.

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

([25]) Delegierte Verordnung (EU) Nr. 1271/2013 der Kommission vom 30. September 2013 über die Rahmenfinanzregelung für Einrichtungen gemäß Artikel 208 der Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates (ABl. L 328 vom 7.12.2013, S. 42).

(5) Das Jahresarbeitsprogramm enthält detaillierte Ziele und Angaben zu den erwarteten Ergebnissen, einschließlich Erfolgsindikatoren. Es enthält zudem eine Beschreibung der zu finanzierenden Maßnahmen sowie Angaben zur Höhe der für die einzelnen Maßnahmen vorgesehenen finanziellen und personellen Ressourcen gemäß den Grundsätzen der maßnahmenbezogenen Aufstellung des Haushaltsplans und des maßnahmenbezogenen Managements. Das Jahresarbeitsprogramm muss mit dem mehrjährigen Arbeitsprogramm nach Absatz 7 im Einklang stehen. Es ist klar darin anzugeben, welche Aufgaben im Vergleich zum vorangegangenen Haushaltsjahr hinzugefügt, verändert oder gestrichen wurden.

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

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

(8) Die Ressourcenplanung wird jährlich aktualisiert. Die strategische Programmplanung ist zu aktualisieren, wann immer dies geboten erscheint und insbesondere, wenn dies notwendig ist, um dem Ergebnis der in Artikel 67 genannten Bewertung Rechnung zu tragen.

Artikel 25

Interessenerklärung

(1) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und die von den Mitgliedstaaten auf Zeit abgeordneten Beamten geben eine Verpflichtungserklärung und eine Interessenerklärung ab, aus der hervorgeht, ob direkte oder indirekte Interessen bestehen, die ihre Unabhängigkeit beeinträchtigen könnten. Die Erklärungen müssen der Wahrheit entsprechen und vollständig sein; sie werden jedes Jahr schriftlich abgegeben und, wann immer erforderlich, aktualisiert.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und externe Sachverständige, die in den Ad-hoc-Arbeitsgruppen mitwirken, geben spätestens zu Beginn jeder Sitzung eine wahrheitsgetreue und vollständige Erklärung über alle Interessen ab, die ihre Unabhängigkeit in Bezug auf die Tagesordnungspunkte beeinträchtigen könnten, und beteiligen sich nicht an den Diskussionen und den Abstimmungen über solche Punkte.

(3) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten der Vorschriften über Interessenerklärungen nach den Absätzen 1 und 2 fest.

Artikel 26

Transparenz

(1) Die ENISA übt ihre Tätigkeiten mit einem hohen Maß an Transparenz und im Einklang mit Artikel 28 aus.

(2) Die ENISA stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu ihren eigenen Arbeitsergebnissen, erhalten. Ferner veröffentlicht sie die nach Artikel 25 abgegebenen Interessenerklärungen.

(3) Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Tätigkeiten der ENISA teilnehmen.

(4) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Transparenzregelungen fest.

Artikel 27

Vertraulichkeit

(1) Unbeschadet des Artikels 28 gibt die Agentur Informationen, die bei ihr eingehen oder von ihr verarbeitet werden und die auf begründetes Ersuchen vertraulich behandelt werden sollen, nicht an Dritte weiter.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die Mitglieder der ENISA-Beratungsgruppe, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal der ENISA, einschließlich der von den Mitgliedstaaten auf Zeit abgeordneten Beamten, unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 AEUV.

(3) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Vertraulichkeitsregelungen fest.

(4) Soweit es zur Erfüllung der Aufgaben der ENISA erforderlich ist, beschließt der Verwaltungsrat, die ENISA zum Umgang mit Verschlusssachen zu ermächtigen. In diesem Fall nimmt die ENISA im Einvernehmen mit den Dienststellen der Kommission Sicherheitsvorschriften zur Anwendung der Sicherheitsgrundsätze an, die in den Beschlüssen (EU, Euratom) 2015/443 ([26]) und (EU, Euratom) 2015/444 ([27]) der Kommission festgelegt sind. Diese Sicherheitsvorschriften betreffen unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung von Verschlusssachen.

Artikel 28

Zugang zu Dokumenten

(1) Die Verordnung (EG) Nr. 1049/2001 findet Anwendung auf die Dokumente der ENISA.

(2) Der Verwaltungsrat legt bis zum 28. Dezember 2019 Maßnahmen zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

(3) Gegen Entscheidungen der ENISA gemäß Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe des Artikels 228 AEUV bzw. 263 AEUV Beschwerde beim Europäischen Bürgerbeauftragten eingelegt oder Klage beim Gerichtshof der Europäischen Union erhoben werden.

KAPITEL IV

Aufstellung und Gliederung des Haushaltsplans der ENISA

Artikel 29

Aufstellung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr und übermittelt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans vor. Einnahmen und Ausgaben müssen ausgeglichen sein.

(2) Der Verwaltungsrat erstellt jedes Jahr auf der Grundlage des Entwurfs des Voranschlags einen Voranschlag der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr.

(3) Der Verwaltungsrat übermittelt jedes Jahr bis zum 31. Januar der Kommission und den Drittländern, mit denen die Union Abkommen nach Artikel 42 Absatz 2 geschlossen hat, den Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments ist.

(4) Die Kommission setzt aufgrund dieses Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan und den Betrag des Zuschusses aus dem Gesamthaushaltsplan der Union in den Haushaltsplanentwurf der Union ein, den sie nach Artikel 314 AEUV dem Europäischen Parlament und dem Rat vorlegt.

(5) Das Europäische Parlament und der Rat bewilligen die Mittel für den Beitrag der Union für die ENISA.

(6) Das Europäische Parlament und der Rat legen den Stellenplan der ENISA fest.

([26]) Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

([27]) Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

(7) Der Haushaltsplan der ENISA wird zusammen mit dem einheitlichen Programmplanungsdokument vom Verwaltungsrat angenommen. Der Haushaltsplan der ENISA wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Erforderlichenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans der ENISA und des einheitlichen Programmplanungsdokuments entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 30

Gliederung des Haushaltsplans der ENISA

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

a) ein Beitrag aus dem Gesamthaushalt der Union;

b) Einnahmen, die konkreten Ausgabenpositionen im Einklang mit der in Artikel 32 genannten Finanzregelung zugewiesen werden;

c) Unionsmittel in Form von Übertragungsvereinbarungen oder Ad-hoc-Finanzhilfen im Einklang mit der in Artikel 32 genannten Finanzregelung der Agentur und den Bestimmungen der einschlägigen Instrumente zur Unterstützung der Unionspolitik;

d) Beiträge von Drittländern, die sich nach Artikel 42 an der Arbeit der ENISA beteiligen;

e) freiwillige Zahlungen oder Sachleistungen von Mitgliedstaaten.

Mitgliedstaaten, die einen freiwilligen Beitrag nach Unterabsatz 1 Buchstabe e leisten, können aufgrund dessen keine bestimmten Rechte oder Dienstleistungen beanspruchen.

(2) Die Ausgaben der ENISA umfassen Aufwendungen für Personal, Verwaltung, technische Unterstützung, Infrastruktur, Betriebskosten und Ausgaben, die sich aus Verträgen mit Dritten ergeben.

Artikel 31

Ausführung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor trägt die Verantwortung für die Ausführung des Haushaltsplans der ENISA.

(2) Der interne Rechnungsprüfer der Kommission übt gegenüber der ENISA dieselben Befugnisse wie gegenüber den Kommissionsdienststellen aus.

(3) Bis zum 1. März des jeweils folgenden Haushaltsjahres (1. März des Jahres n+1) übermittelt der Rechnungsführer der Agentur dem Rechnungsführer der Kommission und dem Rechnungshof den vorläufigen Jahresabschluss für das Haushaltsjahr (Jahr n).

(4) Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Jahresabschluss der ENISA gemäß Artikel 246 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates ([28]), erstellt der Rechnungsführer in eigener Verantwortung den endgültigen Jahresabschluss der ENISA und legt ihn dem Verwaltungsrat zur Stellungnahme vor.

(5) Der Verwaltungsrat gibt eine Stellungnahme zu den endgültigen Jahresabschlüssen der ENISA ab.

(6) Bis zum 31. März des Jahres n+1 übermittelt der Exekutivdirektor den Bericht über die Haushaltsführung und das Finanzmanagement dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof.

(7) Bis zum 1. Juli des Jahres n+1 übermittelt der Rechnungsführer der ENISA den endgültigen Jahresabschluss zusammen mit der Stellungnahme des Verwaltungsrats dem Europäischen Parlament, dem Rat, dem Rechnungsführer der Kommission und dem Rechnungshof.

([28]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

(8) Gleichzeitig mit der Übermittlung des endgültigen Jahresabschlusses der ENISA leitet der Rechnungsführer der ENISA auch dem Rechnungshof eine Erklärung über die Vollständigkeit dieses endgültigen Jahresabschlusses mit Kopie an den Rechnungsführer der Kommission zu.

(9) Bis zum 15. November des Jahres n+1 veröffentlicht der Exekutivdirektor den endgültigen Jahresabschluss im *Amtsblatt der Europäischen Union*.

(10) Bis zum 30. September des Jahres n+1 übermittelt der Exekutivdirektor dem Rechnungshof eine Antwort auf dessen Bemerkungen und leitet eine Kopie dieser Antwort auch dem Verwaltungsrat und der Kommission zu.

(11) Der Exekutivdirektor unterbreitet dem Europäischen Parlament auf dessen Ersuchen nach Artikel 261 Absatz 3 der Verordnung (EU, Euratom) 2018/1046 alle für ein reibungsloses Entlastungsverfahren für das betreffende Haushaltsjahr notwendigen Informationen.

(12) Auf Empfehlung des Rates erteilt das Europäische Parlament dem Direktor vor dem 15. Mai des Jahres n+2 Entlastung zur Ausführung des Haushaltsplans für das Jahr n.

Artikel 32

Finanzregelung

Der Verwaltungsrat erlässt nach Konsultation der Kommission die für die ENISA geltende Finanzregelung. Die Finanzregelung darf von der Delegierten Verordnung (EU) Nr. 1271/2013 nur abweichen, wenn dies für den Betrieb der ENISA eigens erforderlich ist und die Kommission vorher ihre Zustimmung erteilt hat.

Artikel 33

Betrugsbekämpfung

(1) Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates ([29]) tritt die ENISA bis zum 28. Dezember 2019 der Interinstitutionellen Vereinbarung vom 25. Mai 1999 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) ([30]) bei. Die ENISA erlässt die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der ENISA gelten, nach dem Muster im Anhang der genannten Vereinbarung.

(2) Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der ENISA erhalten haben, Rechnungsprüfungen anhand von Belegkontrollen und Kontrollen vor Ort durchzuführen.

(3) Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (EU, Euratom) Nr. 883/2013 und der Verordnung (Euratom, EG) Nr. 2185/96 des Rates ([31]) Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit von der ENISA gewährten Finanzhilfen oder von ihr finanzierten Aufträgen ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

(4) Unbeschadet der Absätze 1, 2 und 3 müssen Kooperationsvereinbarungen mit Drittländern oder internationalen Organisationen, Verträge, Finanzhilfevereinbarungen und Finanzhilfebeschlüsse der ENISA Bestimmungen enthalten, die den Rechnungshof und das OLAF ausdrücklich ermächtigen, derartige Rechnungsprüfungen und Untersuchungen im Rahmen ihrer jeweiligen Zuständigkeiten durchzuführen.

([29]) Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).
([30]) ABl. L 136 vom 31.5.1999, S. 15.
([31]) Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. L 292 vom 15.11.1996, S. 2).

KAPITEL V

Personal

Artikel 34

Allgemeine Bestimmungen

Für das Personal der ENISA gelten das Statut der Beamten, die Beschäftigungsbedingungen für die sonstigen Bediensteten sowie die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung der Bestimmungen des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten.

Artikel 35

Vorrechte und Befreiungen

Das dem EUV und dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf die ENISA und ihr Personal Anwendung.

Artikel 36

Exekutivdirektor

(1) Der Exekutivdirektor wird als Zeitbediensteter der ENISA nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen für die sonstigen Bediensteten eingestellt.

(2) Der Exekutivdirektor wird vom Verwaltungsrat aus einer Liste von Kandidaten, die die Kommission im Anschluss an ein offenes und transparentes Auswahlverfahren vorgeschlagen hat, ernannt.

(3) Beim Abschluss des Arbeitsvertrags des Exekutivdirektors wird die ENISA durch den Vorsitzenden des Verwaltungsrats vertreten.

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

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

(6) Der Verwaltungsrat beschließt über die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors gemäß Artikel 18 Absatz 2.

(7) Der Verwaltungsrat kann auf Vorschlag der Kommission unter Berücksichtigung der Bewertung nach Absatz 5 die Amtszeit des Exekutivdirektors einmal um fünf Jahre verlängern.

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

(9) Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, nimmt nicht an einem anderen Auswahlverfahren für dieselbe Stelle teil.

(10) Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission seines Amtes enthoben werden.

Artikel 37

Abgeordnete nationale Sachverständige und sonstiges Personal

(1) Die ENISA kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht von der ENISA selbst beschäftigt wird. Für dieses Personal gelten das Statut der Beamten und die Beschäftigungsbedingungen für die sonstigen Bediensteten nicht.

(2) Der Verwaltungsrat beschließt eine Regelung über zur ENISA abgeordnete nationale Sachverständige.

KAPITEL VI

Allgemeine Bestimmungen für die ENISA

Artikel 38

Rechtsform der ENISA

(1) Die ENISA ist eine Einrichtung der Union und besitzt Rechtspersönlichkeit.

(2) Die ENISA besitzt in jedem Mitgliedstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach nationalem Recht zuerkannt ist. Sie kann insbesondere bewegliches und unbewegliches Vermögen erwerben oder veräußern und ist vor Gericht parteifähig.

(3) Die ENISA wird vom Exekutivdirektor vertreten.

Artikel 39

Haftung der ENISA

(1) Die vertragliche Haftung der ENISA bestimmt sich nach dem für den betreffenden Vertrag geltenden Recht.

(2) Für Entscheidungen aufgrund einer Schiedsklausel in einem von der ENISA geschlossenen Vertrag ist der Gerichtshof der Europäischen Union zuständig.

(3) Im Bereich der außervertraglichen Haftung ersetzt die ENISA den durch sie selbst oder ihre Bediensteten in Ausübung ihrer Tätigkeit verursachten Schaden nach den allgemeinen Grundsätzen, die den Rechten der Mitgliedstaaten gemeinsam sind.

(4) In Streitsachen über den Schadensersatz gemäß Absatz 3 ist der Gerichtshof der Europäischen Union zuständig.

(5) Die persönliche Haftung der Bediensteten der ENISA gegenüber der ENISA bestimmt sich nach den für die Bediensteten der ENISA geltenden Beschäftigungsbedingungen.

Artikel 40

Sprachenregelung

(1) Für die ENISA gilt die Verordnung Nr. 1 des Rates ([32]). Die Mitgliedstaaten und die anderen von den Mitgliedstaaten benannten Einrichtungen können sich in einer der Amtssprachen der Organe der Union ihrer Wahl an die ENISA wenden und erhalten eine Antwort in dieser Sprache.

(2) Die für die Arbeit der ENISA erforderlichen Übersetzungsdienste werden vom Übersetzungszentrum für die Einrichtungen der Europäischen Union erbracht.

Artikel 41

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch die ENISA unterliegt der Verordnung (EU) 2018/1725.

(2) Der Verwaltungsrat beschließt die Durchführungsvorschriften gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2018/1725. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) 2018/1725 durch die ENISA erforderlich sind, festlegen.

([32]) Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Wirtschaftsgemeinschaft (ABl. 17 vom 6.10.1958, S. 385/58).

Artikel 42

Zusammenarbeit mit Drittländern und internationalen Organisationen

(1) Die ENISA kann mit den zuständigen Behörden von Drittländern und mit internationalen Organisationen zusammenarbeiten, soweit dies zur Verwirklichung der Ziele dieser Verordnung erforderlich ist. Zu diesem Zweck kann die ENISA, nach vorheriger Genehmigung durch die Kommission, Arbeitsvereinbarungen mit den Behörden von Drittländern und internationalen Organisationen treffen. Diese Arbeitsvereinbarungen begründen keine rechtlichen Verpflichtungen für die Union und ihre Mitgliedstaaten.

(2) Die ENISA steht der Beteiligung von Drittländern offen, die entsprechende Übereinkünfte mit der Europäischen Union geschlossen haben. Gemäß den einschlägigen Bestimmungen dieser Übereinkünfte werden Arbeitsvereinbarungen getroffen, die insbesondere Art, Umfang und Form einer Beteiligung dieser Drittländer an der Tätigkeit der ENISA festlegen; hierzu zählen auch Bestimmungen über die Beteiligung an den von der ENISA durchgeführten Initiativen, finanzielle Beiträge und Personal. In Personalfragen müssen derartige Arbeitsvereinbarungen in jedem Fall mit dem Statut der Beamten und den Beschäftigungsbedingungen für die sonstigen Bediensteten vereinbar sein.

(3) Der Verwaltungsrat verabschiedet eine Strategie für die Beziehungen zu Drittländern und internationalen Organisationen in Bezug auf Angelegenheiten, für die die ENISA zuständig ist. Die Kommission stellt durch den Abschluss einer entsprechenden Arbeitsvereinbarung mit dem Exekutivdirektor sicher, dass die ENISA im Rahmen ihres Mandats und des bestehenden institutionellen Rahmens handelt.

Artikel 43

Sicherheitsvorschriften für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen

Nach Konsultation der Kommission legt die ENISA die Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen der Europäischen Union enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443 und 2015/444 festgelegt sind. Die Sicherheitsvorschriften der ENISA enthalten Bestimmungen über den Austausch, die Verarbeitung und die Speicherung derartiger Informationen.

Artikel 44

Sitzabkommen und Arbeitsbedingungen

(1) Die notwendigen Regelungen über die Unterbringung der ENISA in dem Mitgliedstaat, in dem sie ihren Sitz hat, und über die Einrichtungen, die von diesem Mitgliedstaat zur Verfügung zu stellen sind, sowie die besonderen Vorschriften, die im Sitzmitgliedstaat der ENISA für den Exekutivdirektor, die Mitglieder des Verwaltungsrats, das Personal der ENISA und für Familienangehörige dieser Personen gelten, werden in einem Sitzabkommen festgelegt, das nach Billigung durch den Verwaltungsrat zwischen der ENISA und dem Sitzmitgliedstaat geschlossen wird.

(2) Der Sitzmitgliedstaat der ENISA gewährleistet die bestmöglichen Voraussetzungen für das reibungslose Funktionieren der ENISA, unter Berücksichtigung der Erreichbarkeit des Standortes, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten der Mitglieder des Personals.

Artikel 45

Verwaltungskontrolle

Die Tätigkeit der ENISA unterliegt der Aufsicht des Europäischen Bürgerbeauftragten nach Artikel 228 AEUV.

TITEL III

ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 46

Europäischer Zertifizierungsrahmen für die Cybersicherheit

(1) Der europäische Zertifizierungsrahmen für die Cybersicherheit wird geschaffen, um die Voraussetzungen für einen funktionierenden Binnenmarkt zu verbessern, indem die Cybersicherheit in der Union erhöht wird und indem im Hinblick auf die Schaffung eines digitalen Binnenmarkts für IKT-Produkte, -Dienste und -Prozesse ein harmonisierter Ansatz auf Unionsebene für europäische Schemata für die Cybersicherheitszertifizierung ermöglicht wird.

(2) Der europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden und mit dem bescheinigt wird, dass die nach einem solchen Schema bewerteten IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen, um die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen.

Artikel 47

Das fortlaufende Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung

(1) Die Kommission veröffentlicht ein fortlaufendes Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung (im Folgenden „fortlaufendes Arbeitsprogramm der Union"), in dessen Rahmen die strategischen Prioritäten für künftige europäische Schemata für die Cybersicherheitszertifizierung festgelegt werden sollen.

(2) Das fortlaufende Arbeitsprogramm der Union umfasst insbesondere eine Liste der IKT-Produkte, -Dienste und -Prozesse oder Kategorien davon, die von der Aufnahme in ein europäisches Schema für die Cybersicherheitszertifizierung profitieren können.

(3) Die Aufnahme bestimmter IKT-Produkte, -Dienste und -Prozesse oder bestimmter Kategorien davon in das fortlaufende Arbeitsprogramm der Union muss aus einem oder mehreren der folgenden Gründe gerechtfertigt sein:

a) Verfügbarkeit und Entwicklung nationaler Schemata für die Cybersicherheitszertifizierung für bestimmte Kategorien von IKT-Produkten, -Diensten oder -Prozessen, insbesondere im Hinblick auf das Risiko der Fragmentierung;

b) einschlägige Politik oder einschlägiges Recht der Union oder der Mitgliedstaaten;

c) Nachfrage auf dem Markt;

d) Entwicklungen in der Cyberbedrohungslandschaft;

e) Beauftragung mit der Ausarbeitung eines bestimmten möglichen Schemas durch die Europäische Gruppe für die Cybersicherheitszertifizierung.

(4) Die Kommission trägt den Stellungnahmen der Europäischen Gruppe für die Cybersicherheitszertifizierung und der Gruppe der Interessenträger für die Cybersicherheitszertifizierung zum Entwurf des fortlaufenden Arbeitsprogramm der Union gebührend Rechnung.

(5) Das erste fortlaufende Arbeitsprogramm der Union wird spätestens am 28. Juni 2020 vorgelegt. Das fortlaufende Arbeitsprogramm der Union mindestens alle drei Jahre, und bei Bedarf öfter aktualisiert.

Artikel 48

Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung

(1) Die Kommission kann die ENISA damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung auf der Grundlage des fortlaufenden Arbeitsprogramm der Union zu überarbeiten.

(2) In entsprechend begründeten Fällen kann die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung die ENISA damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung, das nicht im fortlaufenden Arbeitsprogramm der Union enthalten ist, zu überarbeiten. Das fortlaufende Arbeitsprogramm der Union wird entsprechend aktualisiert.

Artikel 49

Ausarbeitung, Annahme und Überarbeitung der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Auf Auftrag der Kommission arbeitet die ENISA gemäß Artikel 48 ein mögliches Schema aus, das den in den Artikeln 51, 52und 54 festgelegten Anforderungen genügt.

(2) nach einem Auftrag der Europäischen Gruppe für die Cybersicherheitszertifizierung gemäß Artikel 48 Absatz 2 kann die ENISA ein mögliches Schema ausarbeiten, das den in den Artikeln 51, 52und 54 festgelegten Anforderungen genügt. Lehnt die ENISA einen solchen Auftrag ab, so muss sie dies begründen. Jede Entscheidung, einen Auftrag abzulehnen, wird vom Verwaltungsrat getroffen.

(3) Bei der Ausarbeitung der möglichen Schemata konsultiert die ENISA alle in Frage kommenden Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses.

(4) Für jedes mögliche Schema setzt die ENISA eine Ad-hoc-Arbeitsgruppe nach Artikel 20 Absatz 4 ein, damit sie der ENISA spezifische Beratung und Sachkenntnis bereitstellt.

(5) Die ENISA arbeitet eng mit der Europäischen Gruppe für die Cybersicherheitszertifizierung zusammen. Die Europäische Gruppe für die Cybersicherheitszertifizierung leistet der ENISA Unterstützung und fachliche Beratung bei der Ausarbeitung des möglichen Schemas und gibt eine Stellungnahme zu dem möglichen Schema ab.

(6) Die ENISA berücksichtigt die Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung weitestgehend, bevor sie der Kommission das nach den Absätzen 3, 4 und 5 ausgearbeitete mögliche Schema vorlegt. Diese Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung ist weder bindend, noch hindert das Fehlen einer solchen Stellungnahme die ENISA daran, das mögliche Schema der Kommission vorzulegen.

(7) Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Schemas kann die Kommission Durchführungsrechtsakte erlassen, in denen für IKT-Produkte, -Dienste und -Prozesse, die die Anforderungen der Artikel 51, 52 und 54 erfüllen, ein europäisches Schema für die Cybersicherheitszertifizierung festgelegt wird. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

(8) Die ENISA bewertet mindestens alle fünf Jahre jedes angenommene europäische Schema für die Cybersicherheitszertifizierung, wobei sie die Rückmeldungen seitens der Interessenträger berücksichtigt. Erforderlichenfalls kann die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung die ENISA damit beauftragen, den Prozess der Ausarbeitung eines überarbeiteten möglichen Schemas nach Artikel 48 und nach dem vorliegenden Artikel einzuleiten.

Artikel 50

Website zu europäischen Schemata für die Cybersicherheitszertifizierung

(1) Die ENISA unterhält eine eigene Website, auf der sie über die europäischen Schemata für die Cybersicherheitszertifizierung, die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen — was Information in Bezug auf nicht mehr gültige Schemata für die Cybersicherheitszertifizierung und widerrufene und abgelaufene europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen einschließt — und die Ablage für Links zu den Informationen zur Cybersicherheit gemäß Artikel 55 informiert und für diese wirbt.

(2) Gegebenenfalls sollten auf der Website gemäß Absatz 1 auch die nationalen Cybersicherheitszertifizierungsschemata angegeben werden, die durch ein europäisches Schema für die Cybersicherheitszertifizierung ersetzt wurden.

Artikel 51

Sicherheitsziele der europäischen Schemata für die Cybersicherheitszertifizierung

Es wird ein europäisches Schema für die Cybersicherheitszertifizierung konzipiert, um — soweit zutreffend — mindestens die folgenden Sicherheitsziele zu verwirklichen:

a) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden während des gesamten Lebenszyklus des IKT-Produkts, -Dienstes oder -Prozesses gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff geschützt.

b) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden während des gesamten Lebenszyklus des IKT-Produkts, -Dienstes oder -Prozesses vor Zerstörung, Verlust, Änderung oder Nichtverfügbarkeit — gleich, ob sie zufällig oder unbefugt erfolgt sind — geschützt.

c) Befugte Personen, Programme oder Maschinen haben nur Zugriff auf die Daten, Dienste oder Funktionen, zu denen sie zugangsberechtigt sind.

d) Bekannte Abhängigkeiten und Sicherheitslücken werden ermittelt und dokumentiert.

e) Es wird protokolliert, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt von wem zugegriffen wurde und welche Daten, Funktionen oder Dienste zu welchem Zeitpunkt von wem genutzt oder anderweitig verarbeitet worden sind.

f) Es kann überprüft werden, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt und von wem zugegriffen wurde oder wer zu welchem Zeitpunkt Daten, Dienste oder Funktionen genutzt oder anderweitig verarbeitet hat.

g) Es wird nachgeprüft, dass IKT-Produkte, -Dienste und -Prozesse keine bekannten Sicherheitslücken aufweisen.

h) Bei einem physischen oder technischen Sicherheitsvorfall werden die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht und der Zugang zu ihnen zeitnah wieder hergestellt.

i) Es wird nachgeprüft, dass IKT-Produkte, -Dienste und -Prozesse sind durch Voreinstellungen und Technikgestaltung sicher sind.

j) IKT-Produkte, -Dienste und -Prozesse werden mit aktueller Software und Hardware, die keine allgemein bekannten Sicherheitslücken aufweisen, bereitgestellt und mit Mechanismen für sichere Updates ausgestattet.

Artikel 52

Vertrauenswürdigkeitsstufen der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann für IKT-Produkte, -Dienste und -Prozesse eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ und/oder „hoch“ angeben. Die Vertrauenswürdigkeitsstufe muss in einem angemessenen Verhältnis zu dem mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundenen Risiko im Hinblick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalls stehen.

(2) Europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen beziehen sich auf die jeweilige Vertrauenswürdigkeitsstufe, die im europäischen Schema für die Cybersicherheitszertifizierung angegeben ist, nach dem das europäische Cybersicherheitszertifikat oder die EU-Konformitätserklärung ausgestellt wurde.

(3) Die jeder Vertrauenswürdigkeitsstufe entsprechenden Sicherheitsanforderungen, einschließlich der entsprechenden Sicherheitsfunktionen und der entsprechenden Strenge und Gründlichkeit für die Bewertung, die das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess durchlaufen muss, werden in dem jeweiligen europäischen Schema für die Cybersicherheitszertifizierung festgelegt.

(4) Das Zertifikat oder die EU-Konformitätserklärung nimmt Bezug auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Cybersicherheitsvorfällen besteht.

(5) Ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung für die Vertrauenswürdigkeitsstufe „niedrig“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat oder diese EU-Konformitätserklärung ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, die bekannten grundlegenden Risiken für Sicherheitsvorfälle und Cyberangriffe möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens eine Überprüfung der technischen Dokumentation. Ist eine solche Prüfung nicht geeignet, werden alternative Prüfungen mit gleicher Wirkung durchgeführt;

(6) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „mittel“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, bekannte Cybersicherheitsrisiken und das Risiko von Cybersicherheitsvorfällen und Cyberangriffen seitens Akteuren mit begrenzten Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens Folgendes: eine Überprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen, und die Prüfung, dass die IKT-Produkte, -Dienste und -Prozesse die erforderlichen Sicherheitsfunktionen korrekt durchführen. Falls diese Bewertungstätigkeiten nicht geeignet sind, werden alternative Tätigkeiten mit gleicher Wirkung durchgeführt;

(7) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „hoch“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und dass sie einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, das Risiko von dem neuesten Stand der Technik entsprechenden Cyberangriffen durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführenden Bewertungstätigkeiten beinhaltet das Folgende; eine Nachprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen; eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste und -Prozesse die erforderlichen Sicherheitsfunktionen entsprechend dem neuesten Stand der Technik ordnungsgemäß durchführen, und eine Beurteilung ihrer Widerstandsfähigkeit gegen kompetente Angreifer mittels Penetrationstests Falls diese Bewertungstätigkeiten nicht geeignet sind, alternative Tätigkeiten durchgeführt.

(8) In einem europäischen Schema für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der verwendeten Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden. Jedes Bewertungsniveau entspricht einer der Vertrauenswürdigkeitsstufen und wird durch eine entsprechende Kombination von Vertrauenswürdigkeitskomponenten definiert.

Artikel 53

Selbstbewertung der Konformität

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann die Durchführung einer Selbstbewertung der Konformität unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen zulassen. Die Selbstbewertung der Konformität ist nur für IKT-Produkte, -Dienste und -Prozesse mit niedrigem Risiko erlaubt, die der Vertrauenswürdigkeitsstufe „niedrig“ entsprechen.

(2) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen kann eine EU-Konformitätserklärung ausstellen, die bestätigt, dass die Erfüllung der im Schema festgelegten Anforderungen nachgewiesen wurde. Durch die Ausstellung einer solchen Erklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, -Dienste und -Prozesse die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess den in diesem Schema festgelegten Anforderungen entspricht.

(3) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen hält die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte oder -Dienste mit dem Schema während eines Zeitraums, der im entsprechenden europäischen Schema für die Cybersicherheitszertifizierung festgelegt ist, für die in Artikel 58 genannte nationale Behörde für die Cybersicherheitszertifizierung bereit. Eine Kopie der EU-Konformitätserklärung ist der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorzulegen.

(4) Sofern im Unionsrecht oder im Recht der Mitgliedstaaten nicht anders bestimmt, ist die Ausstellung einer EU-Konformitätserklärung freiwillig.

(5) Die ausgestellte EU-Konformitätserklärung wird in allen Mitgliedstaaten anerkannt.

Artikel 54

Elemente der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung muss mindestens folgende Elemente enthalten:

a) den Gegenstand und Umfang des Zertifizierungsschemas, einschließlich der Art oder Kategorie der erfassten IKT-Produkte, -Dienste und -Prozesse;

b) eine eindeutige Beschreibung des Zwecks des Schemas und der Art und Weise, wie die ausgewählten Normen, Bewertungsmethoden und Vertrauenswürdigkeitsstufen mit den Erfordernissen der vorgesehenen Nutzer des Schemas in Einklang gebracht wurden;

c) eine Bezugnahme auf die für die Bewertung maßgeblichen internationalen, europäischen oder nationalen Normen oder, wenn keine solchen Normen verfügbar oder geeignet sind, auf technische Spezifikationen, die die Auflagen des Anhangs II der Verordnung (EU) Nr. 1025/2012 erfüllen, oder — wenn solche Spezifikationen nicht verfügbar sind — auf die im europäischen Schema für die Cybersicherheitszertifizierung festgelegten technischen Spezifikationen oder Cybersicherheitsanforderungen;

d) gegebenenfalls eine oder mehrere Vertrauenswürdigkeitsstufen;

e) die Angabe, ob eine Selbstbewertung der Konformität im Rahmen des Schemas zulässig ist;

f) falls anwendbar, spezielle oder zusätzliche Anforderungen an die Konformitätsbewertungsstellen, um deren technische Kompetenz für die Evaluierung der Cybersicherheitsanforderungen zu gewährleisten;

g) besondere Bewertungskriterien und -methoden — wie auch Bewertungsarten — für den Nachweis, dass die in Artikel 51 festgelegten Sicherheitsziele eingehalten werden;

h) falls anwendbar, für die Zertifizierung erforderliche Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen oder auf andere Weise zur Verfügung zu stellen hat;

i) Bedingungen für die Verwendung von Siegeln oder Kennzeichen, sofern das Schema solche vorsieht;

j) Vorschriften für die Überwachung der Einhaltung der mit dem europäischen Cybersicherheitszertifikat oder der EU-Konformitätserklärung verbundenen Anforderungen an IKT-Produkte, -Dienste und -Prozesse, einschließlich der Mechanismen für den Nachweis der beständigen Einhaltung der festgelegten Cybersicherheitsanforderungen;

k) falls anwendbar, Bedingungen für die Ausstellung, Aufrechterhaltung, Fortführung und Verlängerung eines europäischen Cybersicherheitszertifikats sowie Bedingungen für die Ausweitung oder Verringerung des Zertifizierungsumfangs;

l) Vorschriften, wie mit IKT-Produkten, -Diensten und -Prozessen zu verfahren ist, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, die aber den Anforderungen des Schemas nicht genügen;

m) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitslücken von IKT-Produkten und -Diensten und -Prozessen;

n) falls anwendbar, Vorschriften für die Konformitätsbewertungsstellen über die Aufbewahrung von Aufzeichnungen;

o) Angabe nationaler oder internationaler Schemata für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten, -Diensten und -Prozessen, Sicherheitsanforderungen, Evaluierungskriterien und -methoden und Vertrauenswürdigkeitsstufen;

p) Inhalt und Format des europäischen Cybersicherheitszertifikats oder der EU-Konformitätserklärungen, die auszustellen sind;

q) die Dauer der Verfügbarkeit der EU-Konformitätserklärung, der technischen Dokumentation und aller weiteren bereitzuhaltenden Informationen des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen;

r) die maximale Gültigkeitsdauer der nach diesem Schema ausgestellten europäischen Cybersicherheitszertifikate;

s) eine Offenlegungspolitik für nach diesem Schema ausgestellte, geänderte oder entzogene europäische Cybersicherheitszertifikate;

t) Bedingungen für die auf Gegenseitigkeit beruhende Anerkennung von Zertifizierungsschemata von Drittländern;

u) falls anwendbar, Regeln für etwaige im Schema vorgesehene Verfahren zur gegenseitigen Begutachtung für die Behörden oder Stellen, die im Einklang mit Artikel 56 Absatz 6 europäische Cybersicherheitszertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Diese Verfahren gelten unbeschadet der gegenseitigen Begutachtung gemäß Artikel 59;

v) Format und Verfahren, die von den Herstellern oder Anbietern von IKT-Produkten, -Diensten und -Prozessen bei der Bereitstellung und Aktualisierung der ergänzenden Informationen zur Cybersicherheit gemäß Artikel 55 zu befolgen sind.

(2) Die für das europäische Schema für die Cybersicherheitszertifizierung festgelegten Anforderungen stehen in Einklang mit allen geltenden rechtlichen Anforderungen, vor allem jenen, die sich aus dem harmonisierten Unionsrecht ergeben.

(3) Soweit dies in einem bestimmten Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung oder eine EU-Konformitätserklärung, die auf der Grundlage eines europäischen Schemas für die Cybersicherheitszertifizierung ausgestellt wurde, dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den Anforderungen jenes Rechtsakts gegeben ist.

(4) Fehlt harmonisiertes Unionsrecht, so kann das Recht der Mitgliedstaaten auch festlegen, dass ein europäisches Schema für die Cybersicherheitszertifizierung dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den gesetzlichen Anforderungen gegeben ist.

Artikel 55

Ergänzende Informationen über die Cybersicherheit von zertifizierten IKT-Produkten, -Diensten und -Prozessen

(1) Hersteller oder Anbieter von zertifizierten IKT-Produkten, -Diensten oder -Prozessen oder von IKT-Produkten, -Diensten und -Prozessen, für die eine EU-Konformitätserklärung ausgestellt wurde, machen folgende ergänzende Cybersicherheitsangaben der Öffentlichkeit zugänglich:

a) Leitlinien und Empfehlungen zur Unterstützung der Endnutzer bei der sicheren Konfiguration, der Installation, der Bereitstellung, dem Betrieb und der Wartung der IKT-Produkte oder -Dienste;

b) Zeitraum, während dessen den Endnutzern eine Sicherheitsunterstützung angeboten wird, insbesondere in Bezug auf die Verfügbarkeit von cybersicherheitsbezogenen Aktualisierungen;

c) Kontaktangaben des Herstellers oder Anbieters und zulässige Verfahren für den Erhalt von Informationen über Sicherheitslücken von Endnutzern und im Bereich der IT-Sicherheit tätigen Wissenschaftlern;

d) Verweis auf Online-Register mit öffentlich offengelegten Sicherheitslücken in Bezug auf das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess und gegebenenfalls relevante Cybersicherheitsratgeber.

(2) Die in Absatz 1 aufgeführten Angaben werden in elektronischer Form bereitgestellt und bleiben mindestens bis zum Ablauf des jeweiligen EU-Cybersicherheitszertifikats oder der EU-Konformitätserklärung verfügbar und werden bei Bedarf aktualisiert.

Artikel 56

Cybersicherheitszertifizierung

(1) Für IKT-Produkte, -Dienste, und -Prozesse die auf der Grundlage eines nach Artikel 49 angenommenen europäischen Schemas für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Einhaltung der Anforderungen dieses Schemas.

(2) Sofern im Unionsrecht oder im Recht der Mitgliedstaaten nicht anders bestimmt, ist die Cybersicherheitszertifizierung freiwillig.

(3) Die Kommission bewertet regelmäßig die Effizienz und Nutzung der angenommenen europäischen Cybersicherheitszertifizierungsschemata sowie die Frage, ob ein bestimmtes europäisches Cybersicherheitszertifizierungsschema durch das einschlägige Unionsrecht verbindlich vorgeschrieben werden soll, um ein angemessenes Maß an Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen in der Union sicherzustellen und das Funktionieren des Binnenmarktes zu verbessern. Die erste Bewertung findet bis zum 31. Dezember 2023 statt und danach nachfolgende Bewertungen finden mindestens alle zwei Jahre statt.

Die Kommission stellt auf der Grundlage der Ergebnisse der Bewertung fest, welche IKT-Produkte, -Dienste und -Prozesse, die unter ein bestehendes Zertifizierungsschema fallen, unter ein verpflichtendes Zertifizierungsschema fallen müssen.

Die Kommission konzentriert sich dabei vorrangig auf die Sektoren, die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführt sind und die spätestens zwei Jahre nach der Annahme des ersten europäischen Cybersicherheitszertifizierungsschemas bewertet werden.

Bei der Vorbereitung der Bewertung verfährt die Kommission wie folgt:

a) Sie berücksichtigt die Auswirkungen der Maßnahmen auf die Hersteller oder Anbieter solcher IKT-Produkte, -Dienste und -Prozesse und auf die Nutzer hinsichtlich der Kosten dieser Maßnahmen und des gesellschaftlichen oder wirtschaftlichen Nutzens, der sich aus dem erwarteten höheren Maß an Sicherheit für die betreffenden IKT-Produkte, -Dienste und -Prozesse ergibt;

b) sie berücksichtigt das Bestehen und die Umsetzung von Rechtsvorschriften der Mitgliedstaaten und von Drittländern;

c) sie führt eine offene, transparente und inklusive Konsultation mit allen relevanten Interessenträgern und mit den Mitgliedstaaten durch;

d) sie berücksichtigt die Umsetzungsfristen sowie die Übergangsmaßnahmen oder -zeiträume und insbesondere in Hinblick auf die möglichen Auswirkungen der Maßnahme auf die Anbieter oder Hersteller von IKT-Produkten, -Diensten und -Prozessen, einschließlich KMU;

e) sie schlägt die schnellste und effizienteste Art und Weise für die Durchführung des Übergangs von freiwilligen zu obligatorischen Zertifizierungsschemata vor.

(4) Die in Artikel 60 genannten Konformitätsbewertungsstellen stellen ein europäisches Cybersicherheitszertifikat nach diesem Artikel mit der Vertrauenswürdigkeitsstufe „niedrig“ oder „mittel“ auf der Grundlage der Kriterien des nach Artikel 49 durch die Kommission angenommenen europäischen Schemas für die Cybersicherheitszertifizierung aus.

(5) Abweichend von Absatz 4 kann in hinreichend begründeten Fällen ein europäisches Schema für die Cybersicherheitszertifizierung vorsehen, dass ein im Rahmen dieses Schemas erteiltes europäisches Cybersicherheitszertifikat nur von einer öffentlichen Stelle auszustellen ist. Bei einer solchen Stelle muss es sich um eine der folgenden Stellen handeln:

a) eine nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 58 Absatz 1;

b) eine als Konformitätsbewertungsstelle akkreditierte öffentliche Stelle nach Artikel 60 Absatz 1.

(6) Ist im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 49 die Vertrauenswürdigkeitsstufe „hoch“ erforderlich, so kann das europäische Cybersicherheitszertifikat nach diesem Schema nur von einer nationalen Behörde für die Cybersicherheitszertifizierung oder in den folgenden Fällen von einer Konformitätsbewertungsstelle ausgestellt werden:

a) wenn die nationale Behörde für die Cybersicherheitszertifizierung zuvor für jedes einzelne, von einer Konformitätsbewertungsstelle ausgestellte europäische Cybersicherheitszertifikat ihre Zustimmung erteilt hat oder

b) wenn die nationale Behörde für die Cybersicherheitszertifizierung die Aufgabe der Ausstellung solcher europäischen Cybersicherheitszertifikate zuvor allgemein einer Konformitätsbewertungsstelle übertragen hat.

(7) Die natürliche oder juristische Person, die ihre IKT-Produkte, -Dienste oder -Prozesse zur Zertifizierung einreicht, hat der in Artikel 58 genannten nationalen Behörde für die Cybersicherheitszertifizierung — sofern diese Behörde die Stelle ist, die das europäische Cybersicherheitszertifikat erteilt — oder der in Artikel 60 genannten Konformitätsbewertungsstelle alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen.

(8) Der Inhaber eines europäischen Cybersicherheitszertifikats informiert die in Absatz 7 genannte Behörde oder Stelle über etwaige später festgestellte Sicherheitslücken oder Unregelmäßigkeiten hinsichtlich der Sicherheit des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses, die sich auf die mit der Zertifizierung verbundenen Anforderungen auswirken könnten. Die Behörde oder Stelle leitet diese Informationen unverzüglich an die betreffende nationale Behörde für die Cybersicherheitszertifizierung weiter.

(9) Ein europäisches Cybersicherheitszertifikat wird für die im jeweiligen europäischen Zertifizierungsschema für Cybersicherheit festgelegte Dauer erteilt und kann verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt sind.

(10) Ein nach diesem Artikel ausgestelltes europäisches Cybersicherheitszertifikat wird in allen Mitgliedstaaten anerkannt.

Artikel 57

Nationale Cybersicherheitszertifizierungsschemata und Cybersicherheitszertifikate

(1) Unbeschadet des Absatzes 3 dieses Artikels werden nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Artikel 49 Absatz 7 erlassenen Durchführungsrechtsakt festgelegt ist. Nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und-Prozesse, die nicht unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bleiben bestehen.

(2) Die Mitgliedstaaten führen keine neuen nationalen Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen ein, die unter ein geltendes europäisches Schema für die Cybersicherheitszertifizierung fallen.

(3) Vorhandene Zertifikate, die auf der Grundlage nationaler Schemata für die Cybersicherheitszertifizierung ausgestellt wurden und unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bleiben bis zum Ende ihrer Geltungsdauer gültig.

(4) Um die Fragmentierung des Binnenmarkts zu vermeiden, unterrichten die Mitgliedstaaten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung über die Absicht zur Ausarbeitung neuer nationaler Schemata für die Cybersicherheitszertifizierung.

Artikel 58

Nationale Behörden für die Cybersicherheitszertifizierung

(1) Jeder Mitgliedstaat benennt eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet oder im Einverständnis mit einem anderen Mitgliedstaat eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung mit Sitz in diesem anderen Mitgliedstaat, als für die Aufsichtsaufgaben im benennenden Mitgliedstaat zuständig.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen der benannten nationalen Behörden für Cybersicherheitszertifizierung mit. Sofern ein Mitgliedstaat mehr als eine Behörde benennt, teilt er der Kommission auch die Aufgaben mit, die diesen Behörden jeweils zugewiesen wurden.

(3) Unbeschadet des Artikels 56 Absatz 5 Buchstabe a und Absatz 6 ist jede nationale Behörde für die Cybersicherheitszertifizierung im Hinblick auf ihre Organisation, Finanzierungsentscheidungen, Rechtsform und Entscheidungsfindung unabhängig von den Stellen, die sie beaufsichtigt.

(4) Die Mitgliedstaaten stellen sicher, dass die Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 von den Aufsichtstätigkeiten nach diesem Artikel streng getrennt sind und dass diese Tätigkeiten unabhängig voneinander durchgeführt werden.

(5) Die Mitgliedstaaten stellen sicher, dass die nationalen Behörden für die Cybersicherheitszertifizierung eine angemessene Ausstattung zur Ausübung ihrer Befugnisse und zur wirksamen und effizienten Wahrnehmung ihrer Aufgaben besitzen.

(6) Im Hinblick auf eine wirksame Durchführung dieser Verordnung ist es angemessen, dass die nationalen Behörden für die Cybersicherheitszertifizierung in der Europäischen Gruppe für die Cybersicherheitszertifizierung in aktiver, wirksamer, effizienter und sicherer Weise mitarbeiten.

(7) Die nationalen Behörden für die Cybersicherheitszertifizierung haben folgende Aufgaben:

a) Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata für die Cybersicherheitszertifizierung gemäß Artikel 54 Absatz 1 Buchstabe j im Hinblick auf die Beobachtung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den Anforderungen der in ihrem jeweiligen Hoheitsgebiet ausgestellten europäischen Cybersicherheitszertifikate in Zusammenarbeit mit anderen zuständigen Marktüberwachungsbehörden;

b) Überwachung und Durchsetzung der Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, die eine Selbstbewertung der Konformität durchführen, insbesondere Überwachung und Durchsetzung der Verpflichtungen dieser Hersteller oder Anbieter nach Artikel 53 Absätze 2 und 3 und nach dem entsprechenden europäischen Schema für die Cybersicherheitszertifizierung;

c) unbeschadet des Artikels 60 Absatz 3 aktive Unterstützung der nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung;

d) Überwachung und Beaufsichtigung der Tätigkeiten der in Artikel 56 Absatz 5 genannten öffentlichen Stellen;

e) gegebenenfalls Ermächtigung der Konformitätsbewertungsstellen nach Artikel 60 Absatz 3 und Beschränkung, Aussetzung oder Widerruf bestehender Ermächtigungen, wenn die Konformitätsbewertungsstellen gegen die Anforderungen dieser Verordnung verstoßen;

f) Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf europäische Cybersicherheitszertifikate, die von der nationalen Behörde für die Cybersicherheitszertifizierung ausgestellt wurden, oder in Bezug auf europäische Cybersicherheitszertifikate, die nach Artikel 56 Absatz 6 von Konformitätsbewertungsstellen ausgestellt wurden, oder in Bezug auf EU-Konformitätserklärungen nach Artikel 53 eingereicht werden, und Untersuchung des Beschwerdegegenstands in angemessenem Umfang, und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;

g) Vorlage eines zusammenfassenden Jahresberichts über die ausgeführten Tätigkeiten gemäß den Buchstaben b, c und d dieses Absatzes oder gemäß Absatz 8 an die ENISA und die Europäische Gruppe für die Cybersicherheitszertifizierung;

h) Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen mit den Anforderungen dieser Verordnung oder mit den Anforderungen bestimmter europäischer Schemata für die Cybersicherheitszertifizierung; und

i) Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung.

(8) Jede nationale Behörde für die Cybersicherheitszertifizierung hat mindestens die folgenden Befugnisse:

a) Sie kann die Konformitätsbewertungsstellen, die Inhaber europäischer Cybersicherheitszertifikate und die Aussteller von EU-Konformitätserklärungen auffordern, ihr sämtliche Auskünfte zu erteilen, die sie für die Erfüllung ihrer Aufgaben benötigt;

b) sie kann Untersuchungen in Form von Rechnungsprüfungen bei den Konformitätsbewertungsstellen, den Inhabern europäischer Cybersicherheitszertifikate und den Ausstellern von EU-Konformitätserklärungen durchführen, um deren Einhaltung der Bestimmungen dieses Titels zu überprüfen;

c) sie kann im Einklang mit dem nationalen Recht geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen, die Inhaber von europäischen Cybersicherheitszertifikaten und die Aussteller von EU-Konformitätserklärungen den Anforderungen dieser Verordnung oder eines europäischen Schemas für die Cybersicherheitszertifizierung genügen;

d) sie erhält Zugang zu den Räumlichkeiten von Konformitätsbewertungsstellen und von Inhabern europäischer Cybersicherheitszertifikate zum Zweck der Durchführung von Untersuchungen im Einklang mit den Verfahrensvorschriften der Union oder des Mitgliedstaats;

e) sie kann im Einklang mit dem nationalen Recht europäische Cybersicherheitszertifikate widerrufen, die von den nationalen Behörden für die Cybersicherheitszertifizierung oder europäische Cybersicherheitszertifikate, die nach Artikel 56 Absatz 6 von den Konformitätsbewertungsstellen ausgestellt wurden, wenn diese Zertifikate den Anforderungen dieser Verordnung oder eines europäischen Schemas für die Cybersicherheitszertifizierung nicht genügen;

f) sie kann im Einklang mit dem nationalen Recht Sanktionen nach Artikel 65 verhängen und die unverzügliche Beendigung von Verstößen gegen die in dieser Verordnung festgelegten Verpflichtungen anordnen.

(9) Die nationalen Behörden für die Cybersicherheitszertifizierung arbeiten untereinander und mit der Kommission zusammen, indem sie insbesondere Informationen, Erfahrungen und bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT-Produkten -Diensten und -Prozessen austauschen.

Artikel 59

Gegenseitige Begutachtung

(1) Um in der gesamten Union gleichwertige Standards in Bezug auf die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen zu erreichen, unterliegen die nationalen Behörden für die Cybersicherheitszertifizierung einer gegenseitigen Begutachtung.

(2) Die gegenseitige Begutachtung erfolgt auf der Grundlage fundierter und transparenter Bewertungskriterien und -verfahren und erstreckt sich insbesondere auf die Strukturen, Personalressourcen und Verfahren betreffenden Anforderungen sowie auf Vertraulichkeit und Beschwerden.

(3) Die gegenseitige Begutachtung umfasst die Bewertung folgender Aspekte:

a) gegebenenfalls die Frage, ob bei den Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 eine strenge Trennung der Aufgaben und Zuständigkeiten von den Aufsichtstätigkeiten nach Artikel 58 gewahrt wird und beide Tätigkeiten unabhängig voneinander durchgeführt werden;

b) die Verfahren für die Überwachung und Durchsetzung der Vorschriften für die Beobachtung der Übereinstimmung von IKT-Produkten, -Diensten und -Prozessen mit den europäischen Cybersicherheitszertifikaten nach Artikel 58 Absatz 7 Buchstabe a;

c) die Verfahren für die Überwachung und Durchsetzung der Verpflichtungen der Hersteller und Anbieter von IKT-Produkten -Diensten oder -Prozessen nach Artikel 58 Absatz 7 Buchstabe b;

d) die Verfahren für die Überwachung, Genehmigung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen;

e) gegebenenfalls die Frage, ob das Personal von Behörden oder Stellen, die gemäß Artikel 56 Absatz 6 Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen, über die erforderlichen Sachkenntnisse verfügt.

(4) Die gegenseitige Begutachtung erfolgt durch mindestens zwei nationale Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten und die Kommission, und sie wird mindestens einmal alle fünf Jahre durchgeführt. Die ENISA kann sich an der gegenseitigen Begutachtung beteiligen.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, um einen Plan für die gegenseitige Begutachtung festzulegen, der sich auf einen Zeitraum von mindestens fünf Jahren erstreckt, und darin die Kriterien für die Zusammensetzung des die gegenseitige Begutachtung durchführenden Teams, die Methode für die gegenseitige Begutachtung und den Zeitplan, die Häufigkeit und die übrigen damit verbundenen Aufgaben vorzugeben. Beim Erlass dieser Durchführungsrechtsakte trägt die Kommission den Erwägungen der Europäischen Gruppe für die Cybersicherheitszertifizierung angemessen Rechnung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die Europäische Gruppe für die Cybersicherheitszertifizierung prüft die Ergebnisse der gegenseitigen Begutachtung, erstellt eine Zusammenfassung, die der Öffentlichkeit zugänglich gemacht werden kann, und erlässt erforderlichenfalls Leitlinien oder Empfehlungen zu den von den betreffenden Stellen zu ergreifenden Maßnahmen.

Artikel 60

Konformitätsbewertungsstellen

(1) Die Konformitätsbewertungsstellen werden von den nach der Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen akkreditiert. Diese Akkreditierung wird nur ausgestellt, wenn die Konformitätsbewertungsstelle die im Anhang der vorliegenden Verordnung aufgeführten Anforderungen erfüllt.

(2) Hat eine nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 ein europäisches Cybersicherheitszertifikat ausstellt, so wird die Zertifizierungsstelle der nationalen Behörde für die Cybersicherheitszertifizierung nach Absatz 1 des vorliegenden Artikels als Konformitätsbewertungsstelle akkreditiert.

(3) Sind in einem europäischen Schema für die Cybersicherheitszertifizierung spezifische oder zusätzliche Anforderungen gemäß Artikel 54 Absatz 1 Buchstabe f festgelegt, so darf nur solchen Konformitätsbewertungsstellen von der nationalen Behörde für die Cybersicherheitszertifizierung die Befugnis erteilt werden, Aufgaben im Rahmen dieses Schemas wahrzunehmen, die diese Anforderungen einhalten.

(4) Die Akkreditierung nach Absatz 1wird den Konformitätsbewertungsstellen für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen dieses Artikels weiterhin erfüllt. Die nationalen Akkreditierungsstellen treffen innerhalb einer angemessenen Frist alle angebrachten Maßnahmen, um die nach Absatz 1 erteilte Akkreditierung einer Konformitätsbewertungsstelle zu beschränken, auszusetzen oder zu widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

Artikel 61

Notifikation

(1) Für jedes europäische Schema für die Cybersicherheitszertifizierung notifizieren die nationalen Behörden für die Cybersicherheitszertifizierung der Kommission die Konformitätsbewertungsstellen, die für die Erteilung von Zertifikaten entsprechend den in Artikel 52 genannten Vertrauenswürdigkeitsstufen akkreditiert und gegebenenfalls nach Artikel 60 Absatz 3 ermächtigt wurden. Die nationalen Behörden für die Cybersicherheitszertifizierung teilt der Kommission etwaige diesbezügliche Änderungen unverzüglich mit.

(2) Ein Jahr nach Inkrafttreten eines europäischen Schemas für die Cybersicherheitszertifizierung veröffentlicht die Kommission im *Amtsblatt der Europäischen Union* eine Liste der nach diesem Schema notifizierten Konformitätsbewertungsstellen.

(3) Geht der Kommission nach Ablauf der in Absatz 2 genannten Frist eine Notifikation zu, so veröffentlicht sie die Änderungen der Liste der notifizierten Konformitätsbewertungsstellen innerhalb von zwei Monaten ab dem Zeitpunkt des Eingangs dieser Notifikation im *Amtsblatt der Europäischen Union*.

(4) Eine nationale Behörde für die Cybersicherheitszertifizierung kann bei der Kommission die Streichung einer von dieser Behörde notifizierten Konformitätsbewertungsstelle aus der in Absatz 2 genannten Liste beantragen. Die Kommission veröffentlicht die entsprechenden Änderungen der Liste innerhalb eines Monats ab dem Zeitpunkt, zu dem der Antrag der nationalen Behörde für die Cybersicherheitszertifizierung eingegangen ist, im *Amtsblatt der Europäischen Union*.

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifikationen nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 62

Europäische Gruppe für die Cybersicherheitszertifizierung

(1) Die Europäische Gruppe für die Cybersicherheitszertifizierung wird eingesetzt.

(2) Die Europäische Gruppe für die Cybersicherheitszertifizierung setzt sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertretern anderer einschlägiger nationaler Behörden zusammen. Ein Mitglied der Europäischen Gruppe für die Cybersicherheitszertifizierung darf nicht mehr als zwei Mitgliedstaat vertreten.

(3) Interessenträger und maßgebliche Dritte können zur Teilnahme an den Sitzungen der Europäischen Gruppe für die Cybersicherheitszertifizierung und zur Beteiligung an ihrer Arbeit eingeladen werden.

(4) Die Europäische Gruppe für die Cybersicherheitszertifizierung hat folgende Aufgaben:

a) Sie berät und unterstützt die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung dieses Titels — insbesondere in Bezug auf das fortlaufende Arbeitsprogramm der Union — in politischen Fragen der Cybersicherheitszertifizierung, bei der Koordinierung von Politikkonzepten und bei der Ausarbeitung europäischer Schemata für die Cybersicherheitszertifizierung;

b) sie unterstützt und berät die ENISA bei der Ausarbeitung eines möglichen Schemas nach Artikel 49 und arbeitet hierbei mit der ENISA zusammen;

c) sie gibt nach Artikel 49 eine Stellungnahme zu den von der ENISA vorbereiteten möglichen Schemata ab;

d) sie beauftragt die ENISA mit der Ausarbeitung von möglichen Schemata nach Artikel 48 Absatz 2;

e) sie gibt an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Schemata für die Cybersicherheitszertifizierung ab;

f) sie prüft die einschlägigen Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung und tauscht Informationen über und bewährte Verfahren für Cybersicherheitszertifizierungsschemata aus;

g) sie erleichtert die Zusammenarbeit zwischen den nationalen Behörden für die Cybersicherheitszertifizierung nach diesem Titel im Wege des Kapazitätsaufbaus und des Informationsaustauschs, insbesondere durch die Festlegung von Methoden für einen effizienten Austausch von Informationen über Fragen der Cybersicherheitszertifizierung;

h) sie leistet Unterstützung bei der Anwendung des Mechanismus der gegenseitigen Begutachtung gemäß den Regeln, die in einem europäischen Cybersicherheitszertifizierungsschema nach Artikel 54 Absatz 1 Buchstabe u festgelegt wurden;

i) sie erleichtert die Anpassung europäischer Schemata für die Cybersicherheitszertifizierung an international anerkannte Normen, indem sie unter anderem bestehende europäische Schemata für die Cybersicherheitszertifizierung überprüft und der ENISA erforderlichenfalls Empfehlungen unterbreitet, sich mit den einschlägigen internationalen Normungsorganisationen in Verbindung zu setzen, um Unzulänglichkeiten oder Lücken in verfügbaren international anerkannten Normen anzugehen.

(5) Die Kommission nimmt gemäß Artikel 8 Absatz 1 Buchstabe e die Sekretariatsgeschäfte der Europäischen Gruppe für die Cybersicherheitszertifizierung wahr, und führt mit Unterstützung der ENISA ihren Vorsitz.

Artikel 63

Beschwerderecht

(1) Natürliche und juristische Personen haben das Recht, bei dem Aussteller eines europäischen Cybersicherheitszertifikats oder — wenn sich die Beschwerde gegen ein von einer Konformitätsbewertungsstelle nach Artikel 56 Absatz 6 ausgestelltes europäischen Cybersicherheitszertifikat richtet — bei der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung eine Beschwerde einzulegen.

(2) Die Behörde oder Stelle, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer über den Stand des Verfahrens und die getroffene Entscheidung und informiert den Beschwerdeführer über die Möglichkeit eines wirksamen gerichtlichen Rechtsbehelfs nach Artikel 64.

Artikel 64

Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Bezug auf

a) Entscheidungen einer Behörde oder einer Stelle gemäß Artikel 63 Absatz 1, gegebenenfalls auch in Bezug auf die mangelnde Erteilung, Verweigerung der Erteilung oder Anerkennung eines europäischen Cybersicherheitszertifikats, das diese natürliche oder juristische Person innehat bzw. beantragt hat;

b) Untätigkeit im Anschluss an eine Beschwerde bei einer Behörde oder Stelle gemäß Artikel 63 Absatz 1.

(2) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats eingeleitet, in dem die Behörde oder Stelle, gegen die der Rechtsbehelf gerichtet ist, ihren Sitz hat.

Artikel 65

Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Titel und bei Verstößen gegen die europäischen Schemata für die Cybersicherheitszertifizierung 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 unverzüglich mit und melden ihr etwaige spätere Änderungen.

TITEL IV

SCHLUSSBESTIMMUNGEN

Artikel 66

Ausschussverfahren

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

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 Absatz 4 Buchstabe b der Verordnung (EU) Nr. 182/2011.

Artikel 67

Bewertung und Überarbeitung

(1) Bis zum 28. Juni 2024 und danach alle fünf Jahre bewertet die Kommission die Wirkung, Wirksamkeit und Effizienz der ENISA und ihrer Arbeitsmethoden und prüft, ob das Mandat der ENISA möglicherweise geändert werden muss und welche finanziellen Auswirkungen eine solche Änderung hätte. In der Bewertung werden alle Rückmeldungen an die ENISA in Bezug auf ihre Tätigkeiten berücksichtigt. Gelangt die Kommission zu der Auffassung, dass Ziele, Mandat und Aufgaben der ENISA deren Tätigkeit nicht länger rechtfertigen können, kann sie eine Änderung dieser Verordnung im Hinblick auf die für die ENISA geltenden Bestimmungen vorschlagen.

(2) Die Bewertung erstreckt sich auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III dieser Verordnung im Hinblick auf die Ziele, für IKT-Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit und einen besser funktionierenden Binnenmarkt zu gewährleisten.

(3) Bei der Bewertung wird beurteilt, ob wesentliche Anforderungen an die Cybersicherheit für den Zugang zum Binnenmarkt erforderlich sind, damit keine IKT-Produkte, -Dienste und -Prozesse auf den Unionsmarkt gelangen, die den grundlegenden Anforderungen an die Cybersicherheit nicht entsprechen.

(4) Die Kommission übermittelt bis zum 28. Juni 2024 und danach alle fünf Jahre den Bericht über die Bewertung zusammen mit ihren Schlussfolgerungen dem Europäischen Parlament, dem Rat und dem Verwaltungsrat. Die Ergebnisse des Berichts werden öffentlich bekannt gemacht.

Artikel 68

Aufhebung und Rechtsnachfolge

(1) Die Verordnung (EU) Nr. 526/2013 wird mit Wirkung vom 27. Juni 2019 aufgehoben.

(2) Bezugnahmen auf die Verordnung (EU) Nr. 526/2013 und auf die durch jene Verordnung errichtete ENISA gelten als Bezugnahmen auf die vorliegende Verordnung und auf die durch die vorliegende Verordnung errichtete ENISA.

(3) Die durch die vorliegende Verordnung errichtete ENISA ist in Bezug auf das Eigentum und alle Abkommen, rechtlichen Verpflichtungen, Beschäftigungsverträge, finanziellen Verpflichtungen und Verbindlichkeiten die Rechtsnachfolgerin der durch die Verordnung (EU) Nr. 526/2013 errichteten ENISA. Alle vom Verwaltungsrat und vom Exekutivrat gemäß der Verordnung (EU) Nr. 526/2013 getroffenen Entscheidungen bleiben gültig, sofern sie der vorliegenden Verordnung nicht zuwiderlaufen.

(4) Die ENISA wird zum 27. Juni 2019 für unbegrenzte Zeit errichtet.

(5) Der nach Artikel 24 Absatz 4 der Verordnung (EU) Nr. 526/2013 ernannte Exekutivdirektor bleibt im Amt und übt die Funktion des Exekutivdirektors nach Artikel 20 der vorliegenden Verordnung für die restliche Dauer seiner Amtszeit aus. Die übrigen Bestimmungen seines Vertrags bleiben unverändert.

(6) Die nach Artikel 6 der Verordnung (EU) Nr. 526/2013 ernannten Mitglieder des Verwaltungsrats und ihre Stellvertreter bleiben im Amt und üben die Funktion des Verwaltungsrats nach Artikel 15 der vorliegenden Verordnung für die restliche Dauer ihrer Amtszeit aus.

Artikel 69

Inkrafttreten

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

(2) Die Artikel 58, 60, 61, 63, 64und 65, gelten ab dem 28. Juni 2021.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Straßburg am 17. April 2019.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
A. TAJANI	G. CIAMBA

ANHANG

ANFORDERUNGEN AN KONFORMITÄTSBEWERTUNGSSTELLEN

Konformitätsbewertungsstellen, die akkreditiert werden möchten, müssen folgende Anforderungen erfüllen:

1. Eine Konformitätsbewertungsstelle muss nach nationalem Recht gegründet und mit Rechtspersönlichkeit ausgestattet sein.

2. Bei einer Konformitätsbewertungsstelle muss es sich um einen unabhängigen Dritten handeln, der mit der Einrichtung oder den IKT-Produkten, -Diensten oder -Prozessen, die er bewertet, in keinerlei Verbindung steht.

3. Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte, -Dienste oder -Prozesse bewertet, an deren Entwurf, Herstellung, Bereitstellung, Montage, Verwendung oder Wartung Unternehmen beteiligt sind, die von diesem Verband vertreten werden, kann als Konformitätsbewertungsstelle gelten, sofern ihre Unabhängigkeit sowie die Abwesenheit jedweder Interessenkonflikte nachgewiesen sind.

4. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb des zu bewertenden IKT-Produkts, -Dienstes oder -Prozesses noch Bevollmächtigter einer dieser Parteien sein. Dieses Verbot schließt nicht die Verwendung von bereits einer Konformitätsbewertung unterzogenen IKT-Produkten, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher IKT-Produkte zum persönlichen Gebrauch aus.

5. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder direkt an Entwurf, Herstellung bzw. Bau, Vermarktung, Installation, Verwendung oder Instandsetzung dieser IKT-Produkte, -Dienste oder -Prozesse beteiligt sein, noch die an diesen Tätigkeiten beteiligten Parteien vertreten. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit ihren Konformitätsbewertungstätigkeiten, beeinträchtigen können. Dieses Verbot gilt besonders für Beratungsdienste.

6. Falls eine Konformitätsbewertungsstelle Eigentum einer öffentlichen Stelle oder Einrichtung ist oder von dieser betrieben wird, sind die Unabhängigkeit und die Abwesenheit von Interessenkonflikten zwischen der nationalen Behörde für die Cybersicherheitszertifizierung und der Konformitätsbewertungsstelle sicherzustellen und zu dokumentieren.

7. Die Konformitätsbewertungsstellen müssen sicherstellen, dass die Tätigkeiten ihrer Zweigunternehmen oder Unterauftragnehmer die Vertraulichkeit, Objektivität oder Unparteilichkeit ihrer Konformitätsbewertungstätigkeiten nicht beeinträchtigen.

8. Die Konformitätsbewertungsstellen und ihre Mitarbeiter müssen die Konformitätsbewertungstätigkeiten mit höchster beruflicher Integrität und der erforderlichen fachlichen Kompetenz in dem betreffenden Bereich durchführen; sie dürfen keinerlei Einflussnahme durch Druck oder Vergünstigungen, auch finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse ihrer Konformitätsbewertungsarbeit auswirken könnte, insbesondere keinem Druck und keiner Einflussnahme durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben.

9. Eine Konformitätsbewertungsstelle muss in der Lage sein, die bei der Konformitätsbewertung anfallenden Aufgaben, die ihr mit dieser Verordnung übertragen wurden, auszuführen, unabhängig davon, ob diese Aufgaben von ihr selbst oder in ihrem Namen und unter ihrer Verantwortung ausgeführt werden. Jegliche Unterauftragsvergabe oder die Inanspruchnahme von externem Personal sind angemessen zu dokumentieren, dürfen nicht über Vermittler erfolgen und bedürfen einer schriftlichen Vereinbarung, in der unter anderem Vertraulichkeitsaspekte und Interessenkonflikte geklärt werden. Die betreffende Konformitätsbewertungsstelle übernimmt die volle Verantwortung für die durchgeführten Aufgaben.

10. Eine Konformitätsbewertungsstelle muss jederzeit, für jedes Konformitätsbewertungsverfahren und für jede Art, Kategorie und Unterkategorie von IKT-Produkten -Diensten oder -Prozessen über Folgendes verfügen:

    a) das erforderliche Personal mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;

    b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt wird, um sicherzustellen, dass die Verfahren transparent sind und wiederholt werden können. Sie muss über angemessene Regelungen und Verfahren verfügen, bei denen zwischen den Aufgaben, die sie als nach Artikel 61 notifizierte Stelle wahrnimmt, und ihren anderen Tätigkeiten unterschieden wird;

c) Verfahren zur Durchführung von Tätigkeiten, bei denen die Größe eines Unternehmens, die Branche, in der es tätig ist, seine Struktur, der Grad an Komplexität der jeweiligen Technologie der ICT-Produkte, -Dienste oder -Prozesse und der Umstand, dass es sich um Massenfertigung oder Serienproduktion handelt, gebührend berücksichtigt werden.

11. Eine Konformitätsbewertungsstelle muss über die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben verfügen, die mit der Konformitätsbewertung verbunden sind, und Zugang zu allen benötigten Ausrüstungen und Einrichtungen haben.

12. Die Personen, die für die Durchführung der Konformitätsbewertungstätigkeiten zuständig sind, müssen Folgendes besitzen:

a) eine solide Fach- und Berufsausbildung, die alle Tätigkeiten der Konformitätsbewertung umfasst;

b) eine ausreichende Kenntnis der Anforderungen, die mit den durchzuführenden Konformitätsbewertungen verbunden sind, und die entsprechende Befugnis, solche Bewertungen durchzuführen;

c) angemessene Kenntnis und angemessenes Verständnis der geltenden Anforderungen und Prüfnormen;

d) die Fähigkeit zur Erstellung von Bescheinigungen, Protokollen und Berichten als Nachweis für durchgeführte Konformitätsbewertungen.

13. Die Unparteilichkeit der Konformitätsbewertungsstellen, ihrer obersten Führungsebene, des für Bewertungen zuständigen Personals der Konformitätsbewertungsstelle und ihrer Unterauftragnehmer muss gewährleistet sein.

14. Die Vergütung für die oberste Leitungsebene und das für Bewertungen zuständige Personal der Konformitätsbewertungsstelle darf sich nicht nach der Anzahl der durchgeführten Konformitätsbewertungen oder deren Ergebnissen richten.

15. Die Konformitätsbewertungsstellen müssen eine Haftpflichtversicherung abschließen, sofern die Haftpflicht nicht aufgrund des nationalen Rechts vom Mitgliedstaat übernommen wird oder der Mitgliedstaat selbst unmittelbar für die Konformitätsbewertung verantwortlich ist.

16. Die Konformitätsbewertungsstelle und ihre Mitarbeiter, Gremien, Tochterunternehmen, Unterauftragnehmer und alle verbundenen Stellen oder Mitarbeiter externer Gremien einer Konformitätsbewertungsstelle müssen die Vertraulichkeit wahren, und die Informationen, die sie bei der Durchführung ihrer Konformitätsbewertungsaufgaben nach dieser Verordnung oder nach einer nationalen Vorschrift zur Durchführung dieser Verordnung erhalten, fallen unter die berufliche Schweigepflicht, außer wenn eine Offenlegung aufgrund von Rechtsvorschriften der Union oder des Mitgliedstaats, denen diese Personen unterliegen, erforderlich ist und außer gegenüber den zuständigen Behörden der Mitgliedstaaten, in denen sie ihre Tätigkeiten ausüben. Die Rechte des geistigen Eigentums sind zu schützen. Die Konformitätsbewertungsstelle muss über dokumentierte Verfahren in Bezug auf die Anforderungen dieser Nummer verfügen.

17. Abgesehen von Nummer 16 schließen die Anforderungen dieses Anhangs in keiner Weise der Austausch von technischen Informationen und regulatorischen Leitlinien zwischen einer Konformitätsbewertungsstelle und einer Person, die eine Zertifizierung beantragt oder deren Beantragung in Erwägung zieht, aus.

18. Konformitätsbewertungsstellen müssen ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter und angemessener Geschäftsbedingungen ausüben, wobei sie in Bezug auf Gebühren die Interessen der KMU berücksichtigen.

19. Die Konformitätsbewertungsstellen müssen die Anforderungen der einschlägigen Norm erfüllen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Konformitätsbewertungsstellen, die die Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen vornehmen, harmonisiert ist.

20. Die Konformitätsbewertungsstellen müssen sicherstellen, dass die für die Konformitätsbewertung eingesetzten Prüflabors den Anforderungen der einschlägigen Norm entsprechen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Labors, die Tests durchführen, harmonisiert ist.

Table of correspondence

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)

umgesetzt in:

Cyber-Sicherheitsgesetz; CSG

Inkrafttreten der Umsetzungsmassnahme: *xx. Monat 20xx*

Richtlinie (EU) 2022/2555	**Nationale Umsetzung (CSG):**	**Anmerkungen:**
Artikel 1		
Art. 1 Abs. 2 Bst. a	Art. 12, 18, 19	
Art. 1 Abs. 2 Bst. b	Art. 4 bis 7	
Art. 1 Abs. 2 Bst. c	Art. 13 Abs. 1 Bst. l, n und o	
Art. 1 Abs. 2 Bst. d	Art. 14, 15, 17 und 22	
Artikel 2		
Art. 2 Abs. 1	Art. 1 Abs. 1	
Art. 2 Abs. 2	Art. 1 Abs. 2	
Art. 2 Abs. 3	Art. 1 Abs. 3 Bst. a	
Art. 2 Abs. 4	Art. 1 Abs. 3 Bst. b	
Art. 2 Abs. 7	Art. 1 Abs. 4 Bst. a	
Art. 2 Abs. 10	Art. 1 Abs. 4 Bst. b	
Artikel 3		
Art. 3 Abs. 1	Art. 3 Abs. 2	
Art. 3 Abs. 2	Art. 3 Abs. 3	
Art. 3 Abs. 3	Art. 13 Abs. 1 Bst. e	
Art. 3 Abs. 4	Art. 14 Abs. 2 und 3	
Artikel 4		
Art. 4 Abs. 1	Art. 5 Abs. 5 und Art. 6 Abs. 7	
Artikel 6		
Art. 6 Ziff. 1	Art. 3 Abs. 1 Ziff. 1	
Art. 6 Ziff. 2	Art. 3 Abs. 1 Ziff. 2	
Art. 6 Ziff. 3	Art. 3 Abs. 1 Ziff. 3	

Art. 6 Ziff. 4	Art. 3 Abs. 1 Ziff. 4	
Art. 6 Ziff. 5	Art. 3 Abs. 1 Ziff. 5	
Art. 6 Ziff. 6	Art. 3 Abs. 1 Ziff. 6	
Art. 6 Ziff. 7	Art. 3 Abs. 1 Ziff. 8	
Art. 6 Ziff. 8	Art. 3 Abs. 1 Ziff. 9	
Art. 6 Ziff. 9	Art. 3 Abs. 1 Ziff. 10	
Art. 6 Ziff. 10	Art. 3 Abs. 1 Ziff. 11	
Art. 6 Ziff. 11	Art. 3 Abs. 1 Ziff. 12	
Art. 6 Ziff. 12	Art. 3 Abs. 1 Ziff. 13	
Art. 6 Ziff. 13	Art. 3 Abs. 1 Ziff. 14	
Art. 6 Ziff. 14	Art. 3 Abs. 1 Ziff. 15	
Art. 6 Ziff. 15	Art. 3 Abs. 1 Ziff. 16	
Art. 6 Ziff. 16	Art. 3 Abs. 1 Ziff. 17	
Art. 6 Ziff. 17	Art. 3 Abs. 1 Ziff. 18	
Art. 6 Ziff. 18	Art. 3 Abs. 1 Ziff. 19	
Art. 6 Ziff. 19	Art. 3 Abs. 1 Ziff. 20	
Art. 6 Ziff. 20	Art. 3 Abs. 1 Ziff. 21	
Art. 6 Ziff. 21	Art. 3 Abs. 1 Ziff. 22	
Art. 6 Ziff. 22	Art. 3 Abs. 1 Ziff. 23	
Art. 6 Ziff. 23	Art. 3 Abs. 1 Ziff. 24	
Art. 6 Ziff. 24	Art. 3 Abs. 1 Ziff. 25	
Art. 6 Ziff. 25	Art. 3 Abs. 1 Ziff. 26	
Art. 6 Ziff. 26	Art. 3 Abs. 1 Ziff. 27	
Art. 6 Ziff. 27	Art. 3 Abs. 1 Ziff. 28	
Art. 6 Ziff. 28	Art. 3 Abs. 1 Ziff. 29	
Art. 6 Ziff. 29	Art. 3 Abs. 1 Ziff. 30	
Art. 6 Ziff. 30	Art. 3 Abs. 1 Ziff. 31	
Art. 6 Ziff. 31	Art. 3 Abs. 1 Ziff. 32	
Art. 6 Ziff. 32	Art. 3 Abs. 1 Ziff. 33	
Art. 6 Ziff. 33	Art. 3 Abs. 1 Ziff. 34	
Art. 6 Ziff. 34	Art. 3 Abs. 1 Ziff. 35	
Art. 6 Ziff. 35	Art. 3 Abs. 1 Ziff. 36	
Art. 6 Ziff. 36	Art. 3 Abs. 1 Ziff. 37	

Art. 6 Ziff. 37	Art. 3 Abs. 1 Ziff. 38	
Art. 6 Ziff. 38	Art. 3 Abs. 1 Ziff. 39	
Art. 6 Ziff. 39	Art. 3 Abs. 1 Ziff. 40	
Art. 6 Ziff. 40	Art. 3 Abs. 1 Ziff. 41	
Art. 6 Ziff. 41	Art. 3 Abs. 1 Ziff. 42	
Artikel 7		
Art. 7 Abs. 1	Art. 13 Abs. 1 Bst. p Art. 19 Abs. 1	
Art. 7 Abs. 2	Art. 19	
Art. 7 Abs. 3	Art. 19	
Art. 7 Abs. 4	Art. 19 Abs. 2	
Artikel 8		
Art. 8 Abs. 1	Art. 12 Abs. 1	
Art. 8 Abs. 2	Art. 13 Abs. 1	
Art. 8 Abs. 3	Art. 12 Abs. 2	
Art. 8 Abs. 6		Siehe Internetauftritt https://scs.llv.li
Artikel 9		
Art. 9 Abs. 1	Art. 12 Abs. 3	
Art. 9 Abs. 2	n/a	nur eine Behörde benannt
Art. 9 Abs. 3	Art. 13 Abs. 1 Bst. m	
Art. 9 Abs. 4	Art. 13 Abs. 1 Bst. m	
Art. 9 Abs. 5	Art. 13 Abs. 1 Bst. n	
Artikel 10		
Art. 10 Abs. 1	Art. 13 Abs. 1 Bst. b und Art. 19	
Art. 10 Abs. 3	Art. 18	
Art. 10 Abs. 4	Art. 18 Abs. 1 Bst. g	
Art. 10 Abs. 5	Art. 13 Abs. 1 Bst. r	
Art. 10 Abs. 6	Art. 13 Abs. 1 Bst. n und q	
Art. 10 Abs. 7	Art. 13 Abs. 2 Art. 18 Abs. 1 Bst. k	
Art. 10 Abs. 8	Art. 18 Abs. 1 Bst. k	
Artikel 11		
Art. 11 Abs. 1 und 2	Art. 18	

Art. 11 Abs. 3 Bst. a	Art. 18 Abs. 1 Bst. f	
Art. 11 Abs. 3 Bst. b	Art. 18 Abs. 1 Bst. b	
Art. 11 Abs. 3 Bst. c	Art. 18 Abs. 1 Bst. c	
Art. 11 Abs. 3 Bst. d	Art. 18 Abs. 1 Bst. f	
Art. 11 Abs. 3 Bst. e	Art. 18 Abs. 1 Bst. e	
Art. 11 Abs. 3 Bst. f	Art. 18 Abs. 1 Bst. i	
Art. 11 Abs. 3 Bst. g	Art. 18 Abs. 3	
Art. 11 Abs. 4	Art. 13 Abs. 1 Bst. i Art. 18 Abs. 1 Bst. g	
Art. 11 Abs. 5	Art. 18 Abs. 1 Bst. h	
Artikel 12		
Art. 12 Abs. 1	Art. 18 Abs. 3	
Artikel 13		
Art. 13 Abs. 1 bis 3	n/a	Mit der SCS existiert eine zentrale Stelle
Art. 13 Abs. 4	Art. 13 Abs. 1 Bst. l	
Art. 13 Abs. 5	Art. 13 Abs. 1 Bst. l	
Artikel 14		
Art. 14	Art. 3 Abs. 1 Ziff. 43 Art. 12 Abs. 2 Art. 13 Abs. 1 Bst. n und q	
Artikel 15		
Art. 15	Art. 3 Abs. 1 Ziff. 44 Art. 12 Abs. 2 Art. 18 Abs. 1 Bst. i	
Artikel 16		
Art. 16	Art. 3 Abs. 1 Ziff. 45 Art. 12 Abs. 3 Art. 13 Abs. 1 Bst. n und q	
Artikel 19		
Art. 19	Art. 13 Abs. 1 Bst. r	
Artikel 20		
Art. 20 Abs. 1	Art. 23 Abs. 1, 4 und 6	
Art. 20 Abs. 2	Art. 23 Abs. 2	

Artikel 21		
Art. 21 Abs. 1	Art. 4 Abs. 1 Art. 5 Abs. 1 und 3	
Art. 21 Abs. 2	Art. 5 Abs. 2	
Art. 21 Abs. 3	Art. 5 Abs. 3	
Art. 21 Abs. 4	Art. 5 Abs. 4	
Artikel 23		
Art. 23 Abs. 1	Art. 6 Abs. 1 und 5 Art. 13 Abs. 1 Bst. n	
Art. 23 Abs. 2	Art. 6 Abs. 5	
Art. 23 Abs. 3	Art. 3 Abs. 1 Ziff. 7	
Art. 23 Abs. 4	Art. 6 Abs. 1 Bst. a und b Art. 6 Abs. 2 bis 4	
Art. 23 Abs. 5	Art. 18 Abs. 1 Bst. a und c Art. 13 Abs. 1 Bst. l	
Art. 23 Abs. 6	Art. 13 Abs. 1 Bst. n	
Art. 23 Abs. 7	Art. 7	
Art. 23 Abs. 10	Art. 13 Abs. 1 Bst. l	
Artikel 24		
Art. 24 Abs. 1	Art. 14 Abs. 6	
Artikel 25		
Art. 25 Abs. 1	Art. 13 Abs. 1 Bst. g	
Artikel 27		
Art. 27 Abs. 2	Art. 14 Abs. 2	
Art. 27 Abs. 3	Art. 14 Abs. 3	
Artikel 28		
Art. 28 Abs. 1	Art. 29 Abs. 1 iVm Art. 27 Abs. 1 VLID	
Art. 28 Abs. 2	Art. 29 Abs. 2 iVm Art. 27 Abs. 1 VLID	
Art. 28 Abs. 3	Art. 29 Abs. 4 iVm Art. 28 VLID	
Art. 28 Abs. 4	Art. 29 Abs. 1 iVm Art. 3 Abs. 1 Bst. f VLID	
Art. 28 Abs. 5	Art. 29 Abs. 3 VLID	

Artikel 29		
Art. 29 Abs. 1	Art. 11 Abs. 3 und 4	
Art. 29 Abs. 2	Art. 13 Abs. 1 Bst. i	
Artikel 30		
Art. 30 Abs. 1	Art. 8 Abs. 1	
Artikel 31		
Art. 31 Abs. 1	Art. 13 Abs. 1	
Art. 31 Abs. 2	Art. 13 Abs. 3	
Art. 31 Abs. 3	Art. 13 Abs. 1 Bst. l	
Art. 31 Abs. 4	Art. 14 und Art. 16	
Artikel 32		
Art. 32 Abs. 1	Art. 15	
Art. 32 Abs. 2 Bst. a	Art. 17 Abs. 1 und 2	
Art. 32 Abs. 2 Bst. b	Art. 17 Abs. 1	
Art. 32 Abs. 2 Bst. c	Art. 17 Abs. 1	
Art. 32 Abs. 2 Bst. d	Art. 14 Abs. 7	
Art. 32 Abs. 2 Bst. e	Art. 14 Abs. 1 Bst. a	
Art. 32 Abs. 2 Bst. f	Art. 17 Abs. 1	
Art. 32 Abs. 2 Bst. g	Art. 14 Abs. 1 Bst. b	
Art. 32 Abs. 3	Art. 17	
Art. 32 Abs. 4 Bst. a	Art. 14 Abs. 1	
Art. 32 Abs. 4 Bst. b	Art. 14 Abs. 8	
Art. 32 Abs. 4 Bst. c	Art. 14 Abs. 1	
Art. 32 Abs. 4 Bst. d	Art. 14 Abs. 1 und 2	
Art. 32 Abs. 4 Bst. e	Art. 14 Abs. 4	
Art. 32 Abs. 4 Bst. f	Art. 15 Abs. 1	
Art. 32 Abs. 4 Bst. g	Art. 14 Abs. 5	
Art. 32 Abs. 4 Bst. h	Art. 7	
Art. 32 Abs. 4 Bst. i	Art. 21 Abs. 2 und 3	
Art. 32 Abs. 5	Art. 15 Abs. 5	
Art. 32 Abs. 6	Art. 22, Art. 23 Abs. 3	
Art. 32 Abs. 7	Art. 21 Abs. 5	
Art. 32 Abs. 9	Art. 13 Abs. 1 Bst. l	

Art. 32 Abs. 10	Art. 13 Abs. 1 Bst. l	
Artikel 33		
Art. 33 Abs. 1	Art. 17	
Art. 33 Abs. 2 Bst. a	Art. 17 Abs. 2	
Art. 33 Abs. 2 Bst. b	Art. 17 Abs. 1	
Art. 33 Abs. 2 Bst. c	Art. 16 Bst. c	
Art. 33 Abs. 2 Bst. d	Art. 14 Abs. 1 Bst. a	
Art. 33 Abs. 2 Bst. e	Art. 17 Abs. 1	
Art. 33 Abs. 2 Bst. f	Art. 14 Abs. 1 Bst. b	
Art. 33 Abs. 3	Art. 17	
Art. 33 Abs. 4 Bst. a	Art. 15 Abs. 1	
Art. 33 Abs. 4 Bst. b	Art. 15 Abs. 5	
Art. 33 Abs. 4 Bst. c	Art. 15 Abs. 1	
Art. 33 Abs. 4 Bst. d	Art. 15 Abs. 1 und 2	
Art. 33 Abs. 4 Bst. e	Art. 15 Abs. 3	
Art. 33 Abs. 4 Bst. f	Art. 15 Abs. 1	
Art. 33 Abs. 4 Bst. g	Art. 15 Abs. 5	
Art. 33 Abs. 4 Bst. h	Art. 21 Abs. 2 und 4	
Art. 33 Abs. 6	Art. 13 Abs. 1 Bst. l	
Artikel 34		
Art. 34 Abs. 1	Art. 21 Abs. 2	
Art. 34 Abs. 4	Art. 21 Abs. 3	
Art. 34 Abs. 5	Art. 21 Abs. 4	
Artikel 35		
Art. 35 Abs. 1	Art. 13 Abs. 1 Bst. l	
Artikel 36		
Art. 36	Art. 21	
Artikel 37		
Art. 37 Abs. 1	Art. 13 Abs. 1 Bst. n	
Art. 37 Abs. 2	Art. 17 Abs. 1 und 3	
Artikel 41		
Art. 41 Abs. 1 und 2	Art. 26	