Rat der
Europäischen Union

Brüssel, den 26. November 2021
(OR. en)

14337/21

Interinstitutionelles Dossier:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Rat
Nr. Vordok.:	9583/2/21, 11724/21
Nr. Komm.dok.:	14150/20
Betr.:	Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148 *– Allgemeine Ausrichtung*

I. EINLEITUNG

1. Am 16. Dezember 2020 hat die Kommission den Vorschlag für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (überarbeitete NIS-Richtlinie oder „NIS 2“)[1] angenommen, um die derzeitige Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie)[2] zu ersetzen.

[1] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

[2] 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.

Der Vorschlag war eine der Maßnahmen, die in der Mitteilung „Die Cybersicherheitsstrategie der EU für die digitale Dekade“[3] angekündigt wurden, um zu gewährleisten, dass Bürgerinnen und Bürger sowie Unternehmen von vertrauenswürdigen digitalen Technologien profitieren können.

2. Der Vorschlag beruht auf Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV); Ziel des Vorschlags ist es, die Resilienz und die Kapazitäten zur Reaktion auf Sicherheitsvorfälle öffentlicher und privater Einrichtungen, zuständiger Behörden und der Union als Ganzes weiter zu verbessern.

3. Der für den Vorschlag zuständige Ausschuss im Europäischen Parlament ist der Ausschuss für Industrie, Forschung und Energie (ITRE). Der ITRE-Ausschuss hat den Bericht des Berichterstatters am 28. Oktober 2021 angenommen.

4. Der Europäische Wirtschafts- und Sozialausschuss hat seine Stellungnahme am 28. April 2021 abgegeben.

5. Am 3. Februar 2021 hat der Ausschuss der Ständigen Vertreter beschlossen, den Europäischen Ausschuss der Regionen um Stellungnahme zu dem Vorschlag zu ersuchen[4]. Bislang hat der Europäische Ausschuss der Regionen noch keine Stellungnahme abgegeben.

6. Der Europäische Datenschutzbeauftragte hat seine Stellungnahme am 11. März 2021 abgegeben[5].

7. In seinen Schlussfolgerungen vom 22. März 2021 zur Cybersicherheitsstrategie der EU für die digitale Dekade[6] hat der Rat den auf der NIS-Richtlinie aufbauenden neuen Vorschlag zur Kenntnis genommen und seine Unterstützung für die Stärkung und Harmonisierung der nationalen Cybersicherheitsrahmen und die nachhaltige Zusammenarbeit zwischen den Mitgliedstaaten bekräftigt.

8. In seinen Schlussfolgerungen vom 21./22. Oktober 2021 hat der Europäische Rat dazu aufgerufen, die Beratungen über den Vorschlag für eine überarbeitete NIS-Richtlinie voranzubringen.

---

3 Dok. 14133/20.
4 Dok. 5573/21.
5 Stellungnahme 5/2021 zur Cybersicherheitsstrategie und zur NIS-2-Richtlinie.
6 Dok. 6722/21.

II. BERATUNGEN IN DEN VORBEREITUNGSGREMIEN DES RATES

9. Im Rat wird der Vorschlag von der Horizontalen Gruppe „Fragen des Cyberraums“ (im Folgenden „Gruppe“) geprüft. Die Prüfung des Vorschlags begann unter portugiesischem Vorsitz am 19. Januar mit einer sorgfältigen Durchsicht des Vorschlags, bei der die Mitgliedstaaten ihre Fragen stellen und auf ihre Hauptanliegen hinweisen konnten und von der Kommission genaue Erläuterungen zu den Änderungen in der überarbeiteten Richtlinie erhielten.

10. Unter portugiesischem Vorsitz widmete die Gruppe der Vorlage und der Durchsicht des Vorschlags 17 Sitzungen. Dem Rat (Verkehr, Telekommunikation und Energie) wurde am 4. Juni 2021 ein Sachstandsbericht zu dieser Durchsicht vorgelegt.

11. Unter slowenischem Vorsitz wurden seitdem die Beratungen fortgesetzt und intensiviert; Ziel ist es, auf der Tagung des Rates (Verkehr, Telekommunikation und Energie) am 3. Dezember 2021 eine allgemeine Ausrichtung zu erzielen. Der slowenische Vorsitz hat der Überarbeitung der NIS-2-Richtlinie 15 Sitzungen und zahlreiche bilaterale Beratungen auf allen Ebenen gewidmet.

12. Die Gruppe konzentrierte sich bei ihrer Arbeit auf die Neuformulierung des Textes des Vorschlags, zunächst betreffend die Wechselwirkungen zwischen der NIS-2-Richtlinie und den sektorspezifischen Rechtsvorschriften und den Anwendungsbereich, insbesondere in Bezug auf die öffentliche Verwaltung, DNS-Diensteanbieter und die Ausschlussklausel, sowie anschließend unter anderem betreffend Peer Reviews, gerichtliche Zuständigkeit und Amtshilfe, koordinierte Offenlegung von Schwachstellen, Datenbanken der Domänennamen und Registrierungsdaten sowie internationale Zusammenarbeit.

13. Am 21. September 2021 wurde ein erster Kompromissvorschlag zum Wortlaut der vorgeschlagenen Richtlinie vorgelegt[7], der sich auf die schriftlichen Bemerkungen und Non-Papers der Mitgliedstaaten sowie auf die früheren Kompromissvorschläge betreffend die Wechselwirkungen zwischen der NIS-2-Richtlinie und den sektorspezifischen Rechtsvorschriften und den Anwendungsbereich der NIS-2-Richtlinie stützte.

[7] Dok. 12019/21.

14. Die letzte Überarbeitung[8] des Kompromissvorschlags des Vorsitzes wurde am 22. November 2021 auf Gruppenebene erörtert. Generell begrüßten die Delegationen den Kompromisstext; einige Delegationen äußerten jedoch noch Prüfungsvorbehalte oder Bemerkungen zu Teilen des Kompromissvorschlags. Zu bestimmten Teilen des Textes gab es noch einige fachliche Umformulierungsvorschläge.

III. SACHFRAGEN

15. Auf der Grundlage der Beratungen auf Gruppenebene wurden die folgenden Punkte als die wichtigsten politischen Fragen ermittelt:

a) Anwendungsbereich (Artikel 2)

Seit Beginn der Beratungen über den NIS-2-Vorschlag haben die Mitgliedstaaten vor allem ihre Bedenken hinsichtlich der erheblichen Zunahme der Zahl der unter die Richtlinie fallenden Einrichtungen und insbesondere der Einführung des Schwellenwerts für die Größe zum Ausdruck gebracht, nach der alle mittleren und großen Einrichtungen, die in den Sektoren tätig sind oder die Dienste erbringen, die unter die NIS-2-Richtlinie fallen, in deren Anwendungsbereich fallen. Diese allgemeine Regel wird im Kompromissvorschlag zwar beibehalten, er enthält aber zusätzliche Bestimmungen, um die erforderliche Verhältnismäßigkeit, ein höherwertiges Risikomanagement und eindeutige Kritikalitätskriterien bei der Bestimmung der Einrichtungen, die in den Anwendungsbereich der Richtlinie fallen, zu gewährleisten. Darüber hinaus enthält der Kompromissvorschlag spezifische Bestimmungen über die Priorisierung der Anwendung von Aufsichtsmaßnahmen nach einem risikobasierten Ansatz.

[8] Dok. 12019/5/21 REV 5.

b) Öffentliche Verwaltung (Artikel 2 Absatz 2a)

Die Einbeziehung der öffentlichen Verwaltung in den Anwendungsbereich der NIS-2-Richtlinie war ein kontrovers diskutiertes Thema, da sich der Sektor der öffentlichen Verwaltung stärker von den anderen Sektoren, die unter die NIS-2-Richtlinie fallen, unterscheidet. Der Vorsitz hat sich um einen ausgewogenen Ansatz bemüht, der den Besonderheiten der nationalen Rahmen für die öffentliche Verwaltung Rechnung trägt und den Mitgliedstaaten ein gewisses Maß an Flexibilität bei der Bestimmung der in den Anwendungsbereich der NIS-2-Richtlinie fallenden Einrichtungen der öffentlichen Verwaltung gewährleistet. Im Kompromisstext gilt die NIS-2-Richlinie daher für Einrichtungen der öffentlichen Verwaltung der Zentralregierungen, die Mitgliedstaaten können jedoch auch festlegen, dass die Richtlinie für Einrichtungen der öffentlichen Verwaltung auf regionaler und lokaler Ebene gilt.

c) Ausschlussklausel (Artikel 2 Nummern 3a und 3aa)

Die Mitgliedstaaten wollten die Ausschlussklausel dahingehend weiter präzisieren, dass die Richtlinie nicht für Einrichtungen gilt, die hauptsächlich Tätigkeiten in den Bereichen Verteidigung, nationale Sicherheit, öffentliche Sicherheit oder Strafverfolgung oder aber Tätigkeiten im Zusammenhang mit der nationalen Sicherheit oder Verteidigung ausüben. Die Justiz, Parlamente und Zentralbanken sind ebenfalls ausgeschlossen.

d) Wechselwirkungen mit sektorspezifischen Rechtsvorschriften

Die Mitgliedstaaten betonten die Notwendigkeit einer Angleichung zwischen der NIS-2-Richtlinie und den sektorspezifischen Rechtsvorschriften, insbesondere der Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) und der Richtlinie über die Resilienz kritischer Einrichtungen. Die NIS-2-Richtlinie, die die Grundlage für eine Mindestharmonisierung bei der Cybersicherheit bilden sollte, enthält einen speziellen Artikel zu sektorspezifischen Rechtsakten der Union (Artikel 2b). Was die Wechselwirkungen mit der Richtlinie über die Resilienz kritischer Einrichtungen betrifft, so sorgt der Kompromissvorschlag für mehr Klarheit in Bezug auf den „gefahrenübergreifenden“ Ansatz. Weitere wichtige Ergänzungen betreffen Kooperationsvereinbarungen zwischen den zuständigen Behörden im Rahmen der jeweiligen Rechtsakte.

e) Peer-Learning (Artikel 16)

Von einigen Ausnahmen abgesehen, lehnten die Mitgliedstaaten die Einführung verbindlicher Peer Reviews durch die Kommission ab. Mit dem vorgeschlagenen Kompromiss wird sichergestellt, dass der neue Peer-Learning-Mechanismus auf gegenseitigem Vertrauen aufbaut, auf Freiwilligkeit beruht und von den Mitgliedstaaten gesteuert wird.

f) Gerichtliche Zuständigkeit und Territorialität (Artikel 24) und Amtshilfe (Artikel 34)

Die Mitgliedstaaten haben Bedenken hinsichtlich der Folgen geäußert, die bei unterschiedlicher gerichtlicher Zuständigkeit für Einrichtungen im IKT-Sektor – wie von der Kommission vorgeschlagen – auftreten würden. Mit dem Kompromisstext wurde die gerichtliche Zuständigkeit entsprechend der Art der Einrichtung präzisiert und der Wortlaut zur Amtshilfe gestärkt.

g) Meldepflichten (Artikel 20)

Die Meldepflicht für erhebliche Cyberbedrohungen wurde im Kompromisstext ausgeschlossen, nachdem die Mitgliedstaaten Bedenken geäußert hatten, dass sie die Einrichtungen, die unter die NIS-2-Richtlinie fallen, übermäßig belasten und zu Übermeldungen führen würden.

IV. FAZIT

16. Der Ausschuss der Ständigen Vertreter hat am 24. November 2021 Einvernehmen über den in der Anlage wiedergegebenen Kompromisstext erzielt und beschlossen, ihn dem Rat (Verkehr, Telekommunikation und Energie) zur Festlegung einer allgemeinen Ausrichtung vorzulegen.

17. Der Rat wird daher ersucht, den Kompromisstext des Vorsitzes in der in der Anlage wiedergegebenen Fassung zu billigen und auf seiner Tagung am 3. Dezember 2021 eine allgemeine Ausrichtung festzulegen.

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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

(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[9],

nach Stellungnahme des Ausschusses der Regionen[10],

gemäß dem ordentlichen Gesetzgebungsverfahren,

---

9 ABl. C vom , S. .
10 ABl. C vom , S. .

in Erwägung nachstehender Gründe:

(1) Ziel der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates[11] 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 Cybersicherheitsvorfällen, um so zum reibungslosen Funktionieren der Wirtschaft und Gesellschaft der Union 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 Festlegung 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 sichergestellt. Darüber hinaus hat sie durch die Einrichtung der Kooperationsgruppe[12] und **des** Netzwerks nationaler Reaktionsteams für IT-Sicherheitsvorfälle (CSIRT-Netzwerk)[13] 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.

---

11 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).

12 Artikel 11 der Richtlinie (EU) 2016/1148.

13 Artikel 12 der Richtlinie (EU) 2016/1148.

(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 Bedrohungslage im Bereich der Cybersicherheit 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 Cybersicherheitsvorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Netz- und Informationssystemen dar. Im Ergebnis können Cybersicherheitsvorfälle die Ausübung wirtschaftlicher Tätigkeiten im Binnenmarkt beeinträchtigen, finanzielle Verluste verursachen, das Vertrauen der Nutzer untergraben und der Wirtschaft und Gesellschaft der Union großen Schaden zufügen. Heute sind daher im Bereich Cybersicherheit Vorsorge und Wirksamkeit wichtiger denn je für das reibungslose Funktionieren des Binnenmarkts.

(4) Rechtsgrundlage der Richtlinie (EU) 1148/2016 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 relevante Tätigkeiten ausüben, auferlegt werden, unterscheiden sich von Mitgliedstaat zu Mitgliedstaat erheblich in Bezug auf die Art der Anforderung, ihre Detailliertheit und die Art der Aufsicht. Diese Unterschiede verursachen zusätzliche Kosten und führen zu Schwierigkeiten für Unternehmen, die Waren oder Dienstleistungen 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 diese grenzüberschreitenden Tätigkeiten wesentlich beeinträchtigen.

Darüber hinaus dürfte, insbesondere angesichts des intensiven grenzüberschreitenden Austauschs, eine etwaige suboptimale Gestaltung oder Umsetzung von **Cybersicherheitsmaßnahmen** 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 gab es bei der Umsetzung der in der Richtlinie 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 unterschiedlicher **Maßnahmen** insbesondere die grenzüberschreitende Erbringung von Diensten und das Niveau der Cyberresilienz beeinträchtigen. 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 Sanktionen, 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) **Die** Mitgliedstaaten **sollten in der Lage sein**, die für die Wahrung ihrer wesentlichen Sicherheitsinteressen und den Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit erforderlichen Maßnahmen zu ergreifen und die Ermittlung, Feststellung und Verfolgung von Straftaten zuzulassen [...]. **Für bestimmte öffentliche und private Einrichtungen, die Tätigkeiten in diesen Bereichen ausüben, sollte die Richtlinie nicht gelten. Sie sollte auch nicht für die Tätigkeiten gelten, die Einrichtungen in diesen Bereichen durchführen. Außerdem ist** kein Mitgliedstaat verpflichtet, Auskünfte zu erteilen, deren Preisgabe seinen wesentlichen Sicherheitsinteressen widerspräche. **Nationale oder** Unionsvorschriften zum Schutz von Verschlusssachen, Geheimhaltungsvereinbarungen und informelle Geheimhaltungsvereinbarungen wie das sogenannte Traffic Light Protocol[14] **sind** von Bedeutung.

(6a) Jede Verarbeitung personenbezogener Daten im Rahmen dieser Richtlinie unterliegt dem Unionsrecht betreffend den Schutz personenbezogener Daten und der Privatsphäre. Diese Richtlinie lässt insbesondere die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates unberührt und sollte daher insbesondere nicht die Aufgaben und Befugnisse der unabhängigen Aufsichtsbehörden berühren, die für die Überwachung der Einhaltung des einschlägigen Datenschutzrechts der Union zuständig sind.

---

14 Mithilfe des Traffic Light Protocol (TLP) kann jemand, der Informationen weitergibt, die Empfänger über etwaige Einschränkungen bei der weiteren Verbreitung dieser Informationen informieren. Es wird in fast allen CSIRT-Gemeinschaften und einigen Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres – ISACs) genutzt.

(7) Mit der Aufhebung der Richtlinie (EU) 2016/1148 sollte der Anwendungsbereich nach Sektoren aus den in den Erwägungsgründen 4 bis 6 dargelegten Gründen auf einen größeren Teil der Wirtschaft ausgeweitet werden. Die Liste der Sektoren, die unter die Richtlinie (EU) 2016/1148 fallen, sollte daher erweitert werden, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind. Bei den Vorschriften sollte nicht danach unterschieden werden, ob es sich bei den Einrichtungen um Betreiber wesentlicher Dienste oder um Anbieter digitaler Dienste handelt. Diese Differenzierung hat sich als überholt erwiesen, da sie nicht die tatsächliche Bedeutung der Sektoren oder Dienste für die gesellschaftlichen und wirtschaftlichen Tätigkeiten im Binnenmarkt widerspiegelt.

(8) Gemäß der Richtlinie (EU) 2016/1148 waren die Mitgliedstaaten dafür zuständig zu bestimmen, welche Einrichtungen die Kriterien für die Einstufung als Betreiber wesentlicher Dienste erfüllen („Ermittlungsprozess“). Um die diesbezüglichen großen Unterschiede zwischen den Mitgliedstaaten zu beheben und für alle relevanten Einrichtungen Rechtssicherheit hinsichtlich der Risikomanagementanforderungen und der Meldepflichten 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 mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[15], die in den Sektoren tätig sind oder die Art von Diensten erbringen, die unter die vorliegende Richtlinie fallen, in den Anwendungsbereich der Richtlinie fallen. [...]

---

15 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).

(8a) **Um sicherzustellen, dass über die in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen ein klarer Überblick besteht, sollten die Mitgliedstaaten in der Lage sein, nationale Eigenmeldungsverfahren einzurichten, in deren Rahmen unter diese Richtlinie fallende Einrichtungen verpflichtet sind, den gemäß dieser Richtlinie zuständigen Behörden oder den dafür von den Mitgliedstaaten benannten Stellen zumindest ihren Namen, ihre Anschrift und Kontaktdaten sowie die Branche, in der sie tätig sind, oder die Art der Dienstleistung, die sie erbringen, sowie gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie ihre Dienstleistungen erbringen, zu übermitteln Wenn es auf nationaler Ebene Register gibt, die die Ermittlung der in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen ermöglichen, können die Mitgliedstaaten über die geeigneten Mechanismen entscheiden.**

(9) **Kleinst- oder Kleineinrichtungen**, die bestimmte Kriterien erfüllen, nach denen sie eine Schlüsselrolle für die Wirtschaft oder Gesellschaft des betreffenden Mitgliedstaats oder für bestimmte Sektoren oder Arten von Diensten spielen, **sollten ebenfalls** von der vorliegenden Richtlinie erfasst werden. Die Mitgliedstaaten sollten **dafür** zuständig sein**,** der Kommission **mindestens einschlägige Informationen zu der Zahl der ermittelten Einrichtungen, der Branche, zu der sie gehören, oder der Art der Dienstleistung, die sie erbringen, und die jeweiligen Kriterien, auf deren Grundlage sie ermittelt wurden, zu** übermitteln. **Die Mitgliedstaaten können auch beschließen, der Kommission im Einklang mit den nationalen Sicherheitsvorschriften die Namen dieser Einrichtungen zu übermitteln.**

(9a) **Einrichtungen der öffentlichen Verwaltung, die Tätigkeiten in den Bereichen nationale Sicherheit, Verteidigung, öffentliche Sicherheit, Strafverfolgung sowie der Justiz, der Parlamente und der Zentralbanken ausüben, sind vom Anwendungsbereich dieser Richtlinie ausgenommen. Für die Zwecke dieser Richtlinie gelten Einrichtungen mit Regulierungskompetenz nicht als Einrichtungen, die Tätigkeiten im Bereich der Strafverfolgung ausüben, und sind demnach nicht vom Anwendungsbereich dieser Richtlinie ausgenommen. Außerdem fallen Einrichtungen der öffentlichen Verwaltung einer Zentralregierung, die gemäß einer internationalen Vereinbarung zusammen mit einem Drittland geschaffen wurden, nicht in den Anwendungsbereich dieser Richtlinie.**

(9aa) Die Mitgliedstaaten sollten festlegen können, dass Einrichtungen, die vor Inkrafttreten dieser Richtlinie gemäß der Richtlinie (EU) 2016/1148 als Betreiber wesentlicher Dienste ermittelt wurden, als wesentliche Einrichtungen gelten.

(9aaaa) Diese Richtlinie gilt insofern nicht für diplomatische und konsularische Auslandsvertretungen der Mitgliedstaaten und die von diesen Vertretungen genutzte IKT-Infrastruktur, als sich diese Infrastruktur im Ausland befindet oder für Nutzer im Ausland betrieben wird.

(10) Die Kommission kann in Zusammenarbeit mit der Kooperationsgruppe Leitlinien für die Anwendung der für Klein- und Kleinstunternehmen geltenden Kriterien herausgeben.

(11) **Bei** den in den Anwendungsbereich der vorliegenden Richtlinie fallenden Einrichtungen **werden** zwei Kategorien unterschieden: wesentlich und wichtig**; diese** Einstufung **trägt** dem Grad der Kritikalität des Sektors oder der Art des **erbrachten** Dienstes sowie **der Größe der Einrichtung** Rechnung [...]. **In diesem Zusammenhang sollten gegebenenfalls auch einschlägige branchenspezifische Risikobewertungen oder Leitlinien der zuständigen Behörden gebührend berücksichtigt werden.** Sowohl die wesentlichen als auch die wichtigen Einrichtungen sollten **den** Risikomanagementanforderungen und Meldepflichten unterliegen. Bei den Aufsichts- und Sanktionsregelungen sollte zwischen 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.

(12) **In dieser Richtlinie wird der Ausgangswert für Maßnahmen zum Cybersicherheitsrisikomanagement und Meldepflichten für alle in den Anwendungsbereich der Richtlinie fallenden Sektoren festgelegt. Wenn zusätzliche sektorspezifische Bestimmungen über Maßnahmen zum Cybersicherheitsrisikomanagement und Meldepflichten für notwendig erachtet werden, um ein hohes Maß an Cybersicherheit zu gewährleisten, sollte die Kommission – zur Vermeidung einer Fragmentierung der Cybersicherheitsbestimmungen von Rechtsakten der Union – prüfen, ob diese Bestimmungen im Rahmen der in dieser Richtlinie vorgesehenen Befugnisübertragung in einem Durchführungsrechtsakt festgelegt werden könnten. Sollten sich Durchführungsrechtsakte zu diesem Zweck nicht eignen, so könnten** sektorspezifische Rechtsvorschriften [...] dazu beitragen, **dass** ein hohes Maß an Cybersicherheit gewährleistet **ist** und gleichzeitig den Besonderheiten und Komplexitäten der **betroffenen** Sektoren in vollem Umfang Rechnung getragen **wird**. **Die Gründe dafür, warum ein Durchführungsrechtsakt im Rahmen der in dieser Richtlinie vorgesehenen Befugnisübertragung nicht geeignet ist, sind in den sektorspezifischen Rechtsvorschriften darzulegen. Gleichzeitig sollte im Rahmen solcher sektorspezifischen Bestimmungen von Rechtsakten der Union der Notwendigkeit eines umfassenden und harmonisierten Rahmens für die Cybersicherheit gebührend Rechnung getragen werden.** Die vorliegende Richtlinie berührt nicht die bestehenden Durchführungsbefugnisse, die der Kommission in einer Reihe von Sektoren, darunter Verkehr und Energie, übertragen wurden.

(12a) Wenn wesentliche oder wichtige Einrichtungen nach den Bestimmungen eines sektorspezifischen Rechtsakts der Union zu Maßnahmen verpflichtet sind, die den in dieser Richtlinie festgelegten Verpflichtungen bezüglich des Cybersicherheitsrisikomanagements und der Meldung erheblicher Sicherheitsvorfälle oder erheblicher Cyberbedrohungen in ihrer Wirkung zumindest gleichwertig sind, so sollten diese sektorspezifischen Bestimmungen, einschließlich der Bestimmungen über die Aufsicht und Durchsetzung, zur Anwendung kommen. Bei der Entscheidung, ob in den sektorspezifischen Bestimmungen eines Rechtsakts der Union festgelegte Verpflichtungen in ihrer Wirkung gleichwertig sind, werden die folgenden Aspekte berücksichtigt: i) Die Maßnahmen zum Cybersicherheitsrisikomanagement sollten geeignete und verhältnismäßige technische und organisatorische Maßnahmen zur Beherrschung der Risiken für die Sicherheit der von den einschlägigen Einrichtungen bei der Erbringung ihrer Dienste genutzten Netz- und Informationssysteme sowie mindestens alle in dieser Richtlinie festgelegten Elemente umfassen. ii) Die Verpflichtung zur Meldung erheblicher Sicherheitsvorfälle und Cyberbedrohungen sollte in Bezug auf den Inhalt, das Format und die Übermittlungsfristen der Meldungen mindestens den in dieser Richtlinie festgelegten Verpflichtungen entsprechen. iii) Die in sektorspezifischen Rechtsakten der Union festgelegten Modalitäten für Meldungen durch Einrichtungen und zuständige Behörden sollten den in dieser Richtlinie festgelegten Anforderungen in Bezug auf Inhalt, Format und Fristen mindestens gleichwertig sein und der Rolle der CSIRTs Rechnung tragen. iv) Die für die zuständigen Behörden geltende Verpflichtung zur grenzübergreifenden Zusammenarbeit sollte der in dieser Richtlinie festgelegten Verpflichtung mindestens gleichwertig sein. Wenn die sektorspezifischen Bestimmungen eines Rechtsakts der Union nicht für alle in den Anwendungsbereich dieser Richtlinie fallenden Unternehmen einer bestimmten Branche gelten, sollten die einschlägigen Bestimmungen dieser Richtlinie weiterhin im Falle der Unternehmen zur Anwendung kommen, die nicht unter diese sektorspezifischen Bestimmungen fallen.

(12aa) Die Kommission sollte regelmäßig überprüfen, dass das Erfordernis der gleichwertigen Wirkung in Bezug auf sektorspezifische Bestimmungen zur Anwendung kommt. Bei der Vorbereitung der regelmäßigen Überprüfungen konsultiert die Kommission die Kooperationsgruppe.

(12aaa) Künftige sektorspezifische Rechtsakte der Union sollten den Begriffsbestimmungen in Artikel 4 dieser Richtlinie und dem in Kapitel VI dieser Richtlinie festgelegten Aufsichts- und Durchsetzungsrahmen gebührend Rechnung tragen.

(12ab) Wenn wesentliche oder wichtige Einrichtungen nach sektorspezifischen Bestimmungen von Rechtsakten der Union zu Maßnahmen verpflichtet sind, die den in dieser Richtlinie festgelegten Meldepflichten in ihrer Wirkung zumindest gleichwertig sind, sollte vermieden werden, dass sich Meldepflichten überschneiden, und dafür gesorgt werden, dass Meldungen zu Cyberbedrohungen oder Sicherheitsvorfällen einheitlich und wirksam bearbeitet werden. Zu diesem Zweck kann den Mitgliedstaaten im Rahmen dieser sektorspezifischen Bestimmungen die Möglichkeit eingeräumt werden, ein gemeinsames, automatisches und direktes Meldeverfahren einzurichten, in dessen Rahmen erhebliche Sicherheitsvorfälle und Cyberbedrohungen sowohl den Behörden, deren Aufgaben in den jeweiligen sektorspezifischen Bestimmungen festgelegt sind, als auch den zuständigen Behörden, gegebenenfalls einschließlich der zentralen Anlaufstelle und der CSIRTs, gemeldet werden, die für die in dieser Richtlinie vorgesehenen Aufgaben im Bereich der Cybersicherheit zuständig sind, oder einen Mechanismus einzurichten, mit dem ein systematischer und sofortiger Informationsaustausch und die Zusammenarbeit zwischen den einschlägigen Behörden und den CSIRTs bei der Bearbeitung solcher Meldungen sichergestellt wird. Zur Vereinfachung von Meldungen und zur Umsetzung des gemeinsamen, automatischen und direkten Meldeverfahrens können die Mitgliedstaaten im Einklang mit den sektorspezifischen Rechtsvorschriften die von ihnen gemäß Artikel 11 Absatz 5a dieser Richtlinie eingerichtete zentrale Anlaufstelle nutzen. Im Interesse der Harmonisierung sollten die Meldepflichten sektorspezifischer Rechtsakte der Union den in dieser Richtlinie festgelegten Meldepflichten angeglichen werden. Die Mitgliedstaaten können im Einklang mit den sektorspezifischen Rechtsvorschriften festlegen, dass die nach dieser Richtlinie zuständigen Behörden oder die nationalen CSIRTs die Adressaten der Meldungen sind.

(13) Die Verordnung XXXX/XXXX des Europäischen Parlaments und des Rates sollte im Zusammenhang mit der vorliegenden Richtlinie als sektorspezifischer Rechtsakt der Union in Bezug auf Einrichtungen des Finanzsektors betrachtet werden. Anstelle der Bestimmungen der vorliegenden Richtlinie sollten die Bestimmungen der Verordnung XXXX/XXXX gelten, die sich auf Risikomanagementmaßnahmen im Bereich der Informations- und Kommunikationstechnologie (IKT), das Management und insbesondere die Meldung von 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 Meldepflichten [...] sowie Aufsicht und Durchsetzung beziehen, nicht auf Finanzunternehmen anwenden, die unter die Verordnung XXXX/XXXX 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 XXXX/XXXX zulässig, dass sich [...] die Europäischen Aufsichtsbehörden für den Finanzsektor und die gemäß der Verordnung XXXX/XXXX zuständigen nationalen Behörden an [...] der [...] Arbeit der Kooperationsgruppe beteiligen und mit den gemäß der vorliegenden Richtlinie benannten zentralen Anlaufstellen sowie den nationalen CSIRTs Informationen austauschen und zusammenarbeiten. Die gemäß der Verordnung XXXX/XXXX zuständigen Behörden sollten Einzelheiten zu schwerwiegenden IKT-bezogenen Vorfällen **und erheblichen Cyberbedrohungen** auch an die gemäß der vorliegenden Richtlinie benannten zentralen Anlaufstellen**, zuständigen Behörden oder nationalen CSIRTs** übermitteln. **Dies kann durch automatische und direkte Weiterleitung der Meldungen zu Sicherheitsvorfällen oder über eine gemeinsame Meldeplattform bewerkstelligt werden.** Darüber hinaus sollten die Mitgliedstaaten den Finanzsektor weiterhin in ihre Cybersicherheitsstrategien einbeziehen, und die nationalen CSIRTs **können** den Finanzsektor bei ihren Tätigkeiten einbeziehen.

(13a) Um Lücken und Überschneidungen bei Luftverkehrseinrichtungen gemäß Anhang I Nummer 2 Buchstabe a auferlegten Cybersicherheitsverpflichtungen zu vermeiden, sollten die gemäß den Verordnungen (EG) Nr. 300/2008[16] und (EU) 2018/1139[17] 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 diese Maßnahmen auf nationaler Ebene zusammenarbeiten. Die gemäß den Verordnungen (EG) Nr. 300/2008 und (EU) 2018/1139 benannten nationalen Behörden können davon ausgehen, dass die Einhaltung der Maßnahmen zum Cybersicherheitsrisikomanagement gemäß dieser Richtlinie durch eine Einrichtung den in den genannten Verordnungen festgelegten Anforderungen und den gemäß diesen genannten Verordnungen erlassenen einschlägigen delegierten Rechtsakten und Durchführungsrechtsakten entspricht.

---

16 **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).**

17 **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).**

(14) Angesichts der Zusammenhänge zwischen der Cybersicherheit und der physischen Sicherheit von Einrichtungen sollte dafür gesorgt werden, dass der Ansatz der Richtlinie (EU) XXX/XXX des Europäischen Parlaments und des Rates und der Ansatz der vorliegenden Richtlinie kohärent sind. Um dies zu erreichen, sollten die Mitgliedstaaten sicherstellen, dass kritische Einrichtungen **[**und diesen gleichgestellte Einrichtungen**]** im Sinne der Richtlinie (EU) XXX/XXX als wesentliche Einrichtungen im Sinne der vorliegenden Richtlinie gelten. Die Mitgliedstaaten sollten auch sicherstellen, dass ihre Cybersicherheitsstrategien einen politischen Rahmen für eine verstärkte Koordinierung zwischen der gemäß der vorliegenden Richtlinie zuständigen Behörde und der gemäß Richtlinie (EU) XXX/XXX zuständigen Behörde beim Informationsaustausch über Sicherheitsvorfälle und Cyberbedrohungen und bei der Wahrnehmung von Aufsichtsaufgaben vorsehen. Die gemäß diesen beiden Richtlinien zuständigen Behörden sollten zusammenarbeiten und Informationen austauschen, insbesondere in Bezug auf die Ermittlung kritischer Einrichtungen, Cyberbedrohungen, Cybersicherheitsrisiken**,** Sicherheitsvorfälle **sowie nicht cyberbezogene Risiken, Bedrohungen und Vorfälle**, die kritische Einrichtungen **[oder kritischen Einrichtungen gleichgestellte 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 beiden Richtlinien benannten zuständigen Behörden zu straffen und den Verwaltungsaufwand für die betroffenen Einrichtungen so gering wie möglich zu halten, sollten die zuständigen Behörden zudem bestrebt sein, die Vorlagen für die Meldung von Sicherheitsvorfällen und die Aufsichtsverfahren zu harmonisieren. Die** gemäß der Richtlinie (EU) XXX/XXX zuständigen Behörden **können die** gemäß der vorliegenden Richtlinie zuständigen Behörden **gegebenenfalls ersuchen**, ihre Aufsichts- und Durchsetzungsbefugnisse **in Bezug auf** eine als kritisch eingestufte wesentlichen Einrichtung auszuüben. [...]

(14a) Einrichtungen im Bereich digitale Infrastruktur beruhen im Wesentlichen auf Netz- und Informationssystemen; aus diesem Grund sollte in den Verpflichtungen, die diesen Einrichtungen durch diese Richtlinie im Rahmen ihrer Cybersicherheitsrisikomanagement- und Meldepflichten auferlegt werden, umfassend auf die physische Sicherheit dieser Systeme eingegangen werden. Da diese Angelegenheiten Gegenstand der vorliegende Richtlinie sind, gelten die in den Kapiteln III bis VI der Richtlinie (EU) XXX/XXX [Resilienzrichtlinie] festgelegten Verpflichtungen nicht für solche Einrichtungen.

(15) Die Beibehaltung eines zuverlässigen, resilienten und sicheren Domänennamensystems (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 alle **für den Binnenmarkt wichtigen** Anbieter von DNS-Diensten entlang der **DNS-Bereitstellungs- und -Auflösungskette** gelten, einschließlich **TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Betreiber von** autoritativen Namenservern für Domänennamen und **Betreiber von** rekursiven Resolvern. **Der Begriff „DNS-Diensteanbieter“ sollte nicht für DNS-Dienste gelten, die für die eigenen Zwecke der betreffenden Einrichtung und mit dieser verbundenen Einrichtungen betrieben werden. Die aufgrund dieser Richtlinie für diese Kategorie von Anbietern geltenden Cybersicherheitsverpflichtungen sind streng auf Maßnahmen bezüglich Cybersicherheitsrisikomanagement und Meldungen beschränkt und lassen somit die Steuerung des globalen DNS durch die Multi-Stakeholder-Gemeinschaft unberührt.**

(16) Cloud-Computing-Dienste sollten Dienste umfassen, die auf Abruf und umfassend Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer und verteilter Rechenressourcen ermöglichen. Zu diesen 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 genannten 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, 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 die 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 die 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 die Rechenressourcen zu beschreiben, die sich auf verschiedenen vernetzten Computern oder Geräten befinden und die untereinander durch Nachrichtenaustausch kommunizieren und koordinieren.

(17) Angesichts des Aufkommens innovativer Technologien und neuer Geschäftsmodelle dürften auf dem Markt neue Bereitstellungs- und Dienstmodelle 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.

(18) 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 auch für Anbieter solcher Rechenzentrumsdienste gelten, bei denen es sich nicht um Cloud-Computing-Dienste handelt. Für die Zwecke der vorliegenden Richtlinie sollte der Begriff „Rechenzentrumsdienst“ Dienstleistungen umfassen, mit denen Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von Informationstechnologie 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 ihr für eigene Zwecke betrieben werden.

(19) Anbieter von Postdiensten im Sinne der Richtlinie 97/67/EG des Europäischen Parlaments und des Rates[18] **einschließlich** Anbieter von [...] Kurierdiensten sollten der vorliegenden Richtlinie unterliegen, wenn sie mindestens einen der Schritte in der Postzustellkette und insbesondere Abholung, Sortierung oder Zustellung, einschließlich Abholung durch den Empfänger, anbieten. Transportdienste, die nicht in Verbindung mit einem dieser Schritte erbracht werden, sollten nicht unter Postdienste fallen.

---

18 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).

(20) Diese 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 den Sektoren 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 ihrer Weltraumprogramme 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 Dienstleistungen im gesamten Binnenmarkt haben können. Die COVID-19-Pandemie hat gezeigt, wie anfällig unsere zunehmend interdependenten Gesellschaften für Risiken mit geringer Eintrittswahrscheinlichkeit sind.

(**20a**) **Um ein hohes Maß an Cybersicherheit zu erreichen und aufrechtzuerhalten, sollten die in dieser Richtlinie vorgeschriebenen nationalen Cybersicherheitsstrategien kohärente Steuerungsrahmen für Cybersicherheit umfassen. Diese Strategien können durch ein oder mehrere legislative oder nichtlegislative Dokumente festgelegt sein.**

(21) Angesichts der unterschiedlichen nationalen Governancestrukturen und zwecks Beibehaltung von bereits bestehenden sektorbezogenen Vereinbarungen und Aufsichts- oder Regulierungsstellen der Union sollten die Mitgliedstaaten befugt sein, mehr als eine nationale Behörde zu benennen, die für die Erfüllung der Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen von wesentlichen und wichtigen Einrichtungen gemäß der vorliegenden Richtlinie zuständig sind. Die Mitgliedstaaten sollten diese Funktion einer bestehenden Behörde zuweisen dürfen.

(22) 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 nationale 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.

(23) Einrichtungen sollten den zuständigen Behörden oder den CSIRTs Sicherheitsvorfälle wirksam und effizient melden**, und zwar auch im Hinblick darauf, dass gegebenenfalls rechtzeitig auf Sicherheitsvorfälle reagiert werden kann und damit die meldende Einrichtung eine Antwort erhält**. Die zentralen Anlaufstellen sollten beauftragt werden, die Meldungen über Sicherheitsvorfälle an die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten weiterzuleiten. [...]

(23a) In den sektorspezifischen Rechtsakten der Union, in denen Maßnahmen zum Cybersicherheitsrisikomanagement oder Meldepflichten vorgeschrieben 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 benannten zuständigen Behörden ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf solche Maßnahmen oder Pflichten mit Unterstützung der gemäß der vorliegenden Richtlinie benannten zuständigen Behörden ausüben. Die betroffenen 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 relevanter Informationen zwischen den zuständigen Behörden über Aufsicht und Durchsetzung, wozu auch der Zugang zu Cyberinformationen gehört, der von den gemäß dieser Richtlinie benannten zuständigen Behörden beantragt wird.

(24) Die Mitgliedstaaten sollten über angemessene technische und organisatorische Kapazitäten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen. Die Mitgliedstaaten sollten daher sicherstellen, dass sie über gut funktionierende Reaktionsteams für IT-Sicherheitsvorfälle – Computer Security Incident Response Teams (CSIRTs) oder auch Computer Emergency Response Teams (CERTs) genannt – verfügen, die die grundlegenden Anforderungen erfüllen, damit wirksame und kompatible Kapazitäten zur Bewältigung von Sicherheitsvorfällen und Risiken und eine effiziente Zusammenarbeit auf Unionsebene gewährleistet sind. Um das Vertrauensverhältnis zwischen den Einrichtungen und den CSIRTs zu stärken, **können** [...] die Mitgliedstaaten in Fällen, in denen ein CSIRT Teil der zuständigen Behörde ist, eine funktionale Trennung zwischen den operativen Aufgaben der CSIRTs, insbesondere in Bezug auf den Informationsaustausch und die Unterstützung der Einrichtungen, und den Aufsichtstätigkeiten der zuständigen Behörden in Erwägung ziehen.

(25) In Bezug auf personenbezogene Daten sollten CSIRTs in der Lage sein, im Einklang mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates[19] im Namen und auf Ersuchen einer unter die vorliegende Richtlinie fallenden Einrichtung eine proaktive Überprüfung der für die Bereitstellung ihrer Dienste verwendeten Netz- und Informationssysteme auf Schwachstellen vorzunehmen. Die Mitgliedstaaten sollten **gegebenenfalls** für alle sektorbezogenen CSIRTs ein vergleichbares Niveau an technischen Kapazitäten anstreben. Die Mitgliedstaaten können die Agentur der Europäischen Union für Cybersicherheit (ENISA) um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.

(26) Wegen der Bedeutung der internationalen Zusammenarbeit im Bereich Cybersicherheit sollten die CSIRTs sich zusätzlich zum durch die vorliegende Richtlinie geschaffenen CSIRT-Netzwerk an internationalen Kooperationsnetzen beteiligen können. **Daher können CSIRTs und zuständige Behörden Informationen, einschließlich personenbezogener Daten, mit den CSIRTs oder Behörden von Drittländern zwecks Wahrnehmung ihrer Aufgaben gemäß der Verordnung (EU) 2016/679 austauschen. Wenn weder ein gemäß Artikel 45 der Verordnung (EU) 2016/679 erlassener Angemessenheitsbeschluss noch geeignete Garantien gemäß Artikel 46 der genannten Verordnung vorliegen, kann der Austausch personenbezogener Daten, der für die Eindämmung erheblicher Cyberbedrohungen und die Reaktion auf einen anhaltenden erheblichen Sicherheitsvorfall als notwendig erachtet wird, als wichtiger Grund des öffentlichen Interesses im Sinne des Artikels 49 Absatz 1 Buchstabe d der Verordnung (EU) 2016/679 angesehen werden.**

---

19 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).

(27) Im Einklang mit dem Anhang der Empfehlung (EU) 2017/1548 der Kommission für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen („Konzeptentwurf“)[20] sollte der Begriff „Sicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall bezeichnen, der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt. Je nach Ursache und Auswirkung können sich Sicherheitsvorfälle großen Ausmaßes verschärfen und zu echten Krisen entwickeln, die das reibungslose Funktionieren des Binnenmarkts verhindern. 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.

(28) 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 Cybersicherheitsrisikos. Einrichtungen, die solche Systeme entwickeln **oder verwalten**, sollten daher geeignete Verfahren für die Behandlung von entdeckten Schwachstellen festlegen. Da Schwachstellen häufig von Dritten (meldenden Einrichtungen) entdeckt und gemeldet (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 bzw. die Offenlegung von Schwachstellen. In Bezug auf die Offenlegung von Schwachstellen ist die Koordinierung zwischen meldenden Einrichtungen und Herstellern oder Anbietern von IKT-Produkten oder -Diensten besonders wichtig. Die koordinierte Offenlegung von Schwachstellen erfolgt in einem strukturierten Prozess, in dem den Organisationen Schwachstellen in einer Weise gemeldet werden, die der Organisation 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 Einrichtung und der Organisation in Bezug auf den Zeitplan für die Behebung und Veröffentlichung von Schwachstellen umfassen.

---

20 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).

(29) Die Mitgliedstaaten sollten daher 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 ihrer jeweiligen Rechtsordnung so weit wie möglich die Herausforderungen angehen, mit denen Forschende, die sich mit Schwachstellen befassen, konfrontiert sind, wozu auch deren potenzielle strafrechtliche Haftung gehört.** [...] **D**ie Mitgliedstaaten sollten ein CSIRT benennen, das die Rolle des „Koordinators" übernimmt und gegebenenfalls zwischen den meldenden Einrichtungen und den Herstellern oder Anbietern von IKT-Produkten oder -Diensten vermittelt. Zu den Aufgaben des als Koordinator benannten CSIRT sollte insbesondere gehören, betroffene Einrichtungen zu ermitteln und zu kontaktieren, meldende Einrichtungen zu unterstützen, Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Organisationen betreffen (**koordinierte** Offenlegung von Schwachstellen, die mehrere Parteien betreffen). [...] **Könnte die gemeldete** Schwachstelle **möglicherweise** in mehr als einem Mitgliedstaat **erhebliche Auswirkungen auf Einrichtungen haben** [...], sollten die benannten CSIRTs [...] **gegebenenfalls** im Rahmen des CSIRT-Netzwerkes zusammenarbeiten.

(30) Der rechtzeitige Zugang zu korrekten Informationen über Schwachstellen, die IKT-Produkte und -Dienste beeinträchtigen, trägt zu einem besseren Cybersicherheitsrisikomanagement bei. In dieser Hinsicht sind öffentlich zugängliche Informationen über Schwachstellen nicht nur für Einrichtungen und deren Nutzer, sondern auch für die zuständigen nationalen Behörden und die CSIRTs ein wichtiges Instrument. Aus diesem Grund sollte die ENISA ein Schwachstellenregister einrichten, in dem wesentliche und wichtige Einrichtungen und deren Anbieter sowie, auf freiwilliger Basis, Einrichtungen, die nicht in den Anwendungsbereich der vorliegenden Richtlinie fallen, **und CSIRTs** Schwachstellen offenlegen und Informationen über die Schwachstellen bereitstellen, die es den Nutzern ermöglichen, geeignete Abhilfemaßnahmen zu ergreifen.

(31) 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. Ein von der ENISA gepflegtes europäisches Schwachstellenregister würde für mehr Transparenz in Bezug auf den Prozess der Veröffentlichung vor der offiziellen Offenlegung der Schwachstelle sorgen und die Resilienz im Falle von Störungen oder Unterbrechungen bei der Erbringung ähnlicher Dienste verbessern. Um Doppelarbeit zu vermeiden und im Interesse der größtmöglichen Komplementarität, sollte die ENISA die Möglichkeit prüfen, Vereinbarungen über eine strukturierte Zusammenarbeit mit ähnlichen Registern in Drittländern zu schließen. **Insbesondere sollte die ENISA die Möglichkeit einer engen Zusammenarbeit mit den Betreibern des Systems für bekannte Schwachstellen und Anfälligkeiten (Common Vulnerabilities and Exposures, CVE) prüfen, einschließlich der Möglichkeit, den Status einer Root CVE-Nummerierungsstelle zu erlangen.**

(32) **Die Kooperationsgruppe sollte weiterhin 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 die Maßnahmen aufgeführt sind, die die Gruppe zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen hat. Der Zeitrahmen des ersten Programms, das gemäß der vorliegenden Richtlinie angenommen wird, sollte an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst werden, um etwaige Unterbrechungen der Arbeit der Gruppe zu vermeiden.

(33) 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.

(34) 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 sollte regelmäßige gemeinsame Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union organisieren, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen. Um die Zusammenarbeit auf Unionsebene zu verbessern, sollte die Gruppe in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3), die Agentur der Europäischen Union für Flugsicherheit (EASA) und die Agentur der Europäischen Union für das Weltraumprogramm (EUSPA), zur Teilnahme an ihrer Arbeit einzuladen.

(35) Die zuständigen Behörden und CSIRTs sollten befugt sein, an Austauschprogrammen für Bedienstete aus anderen Mitgliedstaaten teilzunehmen, um die Zusammenarbeit zu verbessern. Die zuständigen Behörden sollten Maßnahmen ergreifen, damit die Bediensteten aus anderen Mitgliedstaaten bei den Tätigkeiten der aufnehmenden zuständigen Behörde konstruktiv mitwirken können.

(35a) Das CSIRT-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 CSIRT-Netzwerk in Erwägung ziehen, mit Cybersicherheitspolitik befasste Einrichtungen und Agenturen der Union, etwa Europol, zur Teilnahme an seiner Arbeit einzuladen.

(36) [...]

(36a) Um die wirksame Umsetzung der Bestimmungen dieser Richtlinie, etwa zum Umgang mit Schwachstellen, zum Cybersicherheitsrisikomanagement, zu Meldemaßnahmen und zu Vereinbarungen über den Informationsaustausch, zu fördern, können die Mitgliedstaaten mit Drittländern zusammenarbeiten und Tätigkeiten durchführen, die für diesen Zweck als angemessen erachtet werden, wozu auch der Informationsaustausch über Bedrohungen, Vorfälle, Schwachstellen, Instrumente und Methoden, Taktiken, Techniken und Verfahren, die Vorsorge und Übungen im Hinblick auf das Cyberkrisenmanagement, Schulungen, die Vertrauensbildung und Vereinbarungen über den strukturierten Informationsaustausch gehören. Solche Kooperationsabkommen sollten mit dem Datenschutzrecht der Union im Einklang stehen.

(37) Die Mitgliedstaaten sollten über die bestehenden Kooperationsnetzwerke – insbesondere das **europäische** Netzwerk der Verbindungsorganisationen für Cyberkrisen (Cyber Crisis Liaison Organisation Network, EU-CyCLONe), das CSIRT-Netzwerk und die Kooperationsgruppe – zur Schaffung des EU-Rahmens für die Reaktion auf Cybersicherheitskrisen gemäß der Empfehlung (EU) 2017/1584 beitragen. EU-CyCLONe und das CSIRT-Netzwerk sollten auf der Grundlage von verfahrenstechnischen Vereinbarungen zusammenarbeiten, in denen die Modalitäten dieser Zusammenarbeit festgelegt werden, **und jegliche Überschneidung von Aufgaben vermeiden**. In der Geschäftsordnung von EU-CyCLONe sollten die Modalitäten für das Funktionieren des Netzwerks genauer festgelegt werden, einschließlich, aber nicht beschränkt auf Funktion und Aufgaben, Formen der Zusammenarbeit, Interaktionen mit anderen relevanten Akteuren und Vorlagen für den Informationsaustausch sowie Kommunikationsmittel. Für das Krisenmanagement auf [...] **Ebene der Unionspolitik** sollten sich die relevanten Parteien auf die Integrierte Regelung für die politische Reaktion auf Krisen (IPCR) 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 (GSVP), so sollte der Krisenreaktionsmechanismus des Europäischen Auswärtigen Dienstes (EAD) ausgelöst werden.

(37a) EU-CyCLONe sollte bei großen Cybersicherheitsvorfällen und -krisen als Vermittlungsinstanz zwischen fachlicher und politischer Ebene fungieren. Das Netzwerk sollte die Zusammenarbeit auf operativer Ebene verbessern, indem es auf den Ergebnissen des CSIRT-Netzwerks aufbaut, eigene Fähigkeiten zur Erstellung von Analysen der Auswirkungen großer Vorfälle und Krisen nutzt und die Entscheidungsfindung auf politischer Ebene unterstützt. Die Organe, Einrichtungen und sonstigen Stellen der EU sollten eine für das Management von großen Sicherheitsvorfällen und -krisen zuständige Behörde benennen, die Mitglied von EU-CyCLONe werden soll.

(38) [...]

(39) [...]

(39a) 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 Sicherheitsmaßnahmen, die den jeweiligen Risiken angemessen sind, umfassen sollte.

(40) Das Risikomanagement sollte **den Grad der Abhängigkeit der Einrichtung von Netz- und Informationssystemen berücksichtigen und** auch Maßnahmen zur Ermittlung jeder Gefahr eines Sicherheitsvorfalls, zur Verhinderung, Aufdeckung und Bewältigung von Sicherheitsvorfällen sowie der Minderung ihrer Folgen umfassen. Die Sicherheit von Netz- und Informationssystemen sollte sich auch auf gespeicherte, übermittelte und verarbeitete Daten erstrecken.

(40a) Da Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, wird in dieser Richtlinie ein „gefahrenübergreifender“ Ansatz angewandt, der den Schutz von Netz- und Informationssystemen und ihres physischen Umfelds vor Ereignissen wie Diebstahl, Feuer, Überschwemmungen und Telekommunikations- oder Stromausfällen oder vor unbefugtem physischen Zugang zu Informationen und Datenverarbeitungsanlagen der Einrichtungen und vor der Schädigung dieser Informationen und Anlagen und den entsprechenden Eingriffen umfasst, 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 sollten daher auch die physische Sicherheit und die Sicherheit des Umfelds berücksichtigt werden, indem Maßnahmen zum Schutz der Netz- und Informationssysteme der Einrichtung vor Systemfehlern, menschlichen Fehlern, böswilligen Handlungen oder natürlichen Phänomenen im Einklang mit europäischen oder international anerkannten Normen, wie denen der Reihe ISO 27000, einbezogen werden. In diesem Zusammenhang sollten sich die Einrichtungen im Rahmen ihrer Risikomanagementmaßnahmen auch mit der Sicherheit des Personals befassen und über angemessene Konzepte für die Zugangskontrolle verfügen. Diese Maßnahmen sollten mit der Richtlinie XXXX [CER-Richtlinie] in Einklang stehen.

(40b) In Ermangelung geeigneter europäischer Systeme für die Cybersicherheitszertifizierung, die gemäß der Verordnung (EU) 2019/881 angenommen wurden, können die Mitgliedstaaten von Einrichtungen verlangen, zertifizierte IKT-Produkte, -Dienste und -Prozesse zu nutzen oder ein Zertifikat im Rahmen verfügbarer nationaler Systeme für die Cybersicherheitszertifizierung zu erlangen, um die Anforderungen an das Cybersicherheitsrisikomanagement gemäß dieser Richtlinie zu erfüllen.

(41) Damit keine unverhältnismäßige finanzielle und administrative Belastung für wesentliche und wichtige Einrichtungen entsteht, sollten die Anforderungen an das Cybersicherheitsrisikomanagement 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 den Kosten für ihre Durchführung** Rechnung getragen. **Die Größe der Einrichtung sowie die Wahrscheinlichkeit des Auftretens von Vorfällen und deren Schweregrad sollten ebenfalls besonders berücksichtigt werden.**

(41a) Um den Regelungsaufwand zu verringern, sollten die Anforderungen an die Umsetzung von Maßnahmen zum Cybersicherheitsrisikomanagement für mittlere und kleine Unternehmen sowie Kleinstunternehmen grundsätzlich weniger streng sein, es sei denn, Kritikalitätskriterien oder nationale Risikobewertungen würden strengere Anforderungen rechtfertigen, insbesondere in Bezug auf Einrichtungen, die die in dieser Richtlinie festgelegten Kritikalitätskriterien erfüllen.

(42) Wesentliche und wichtige Einrichtungen sollten die Sicherheit der bei ihren Tätigkeiten verwendeten Netz- und Informationssysteme gewährleisten. Hauptsächlich handelt es sich dabei um private Netz- und Informationssysteme, die entweder von internem IT-Personal verwaltet werden oder deren Sicherheit Dritten anvertraut wurde. Die Anforderungen an das Cybersicherheitsrisikomanagement und die Meldepflicht gemäß der vorliegenden Richtlinie sollten für die einschlägigen wesentlichen und wichtigen Einrichtungen unabhängig davon gelten, ob sie ihre Netz- und Informationssysteme intern warten oder diese Aufgabe ausgliedern.

(42aa) Angesichts der grenzüberschreitenden Art ihrer Tätigkeit sollte bei DNS-Diensteanbietern, TLD-Namenregistern, Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, Anbietern von Cloud-Computing-Diensten, Anbietern von Rechenzentrumsdiensten, Betreibern von Inhaltszustellnetzen, Anbietern verwalteter Dienste und Anbietern verwalteter Sicherheitsdienste auf Unionsebene eine stärkere Harmonisierung erfolgen. Die Umsetzung von Cybersicherheitsmaßnahmen sollte daher durch einen Durchführungsrechtsakt erleichtert werden.

(43) Besonders wichtig ist die Bewältigung von Cybersicherheitsrisiken, die die Lieferkette von Einrichtungen und deren Beziehungen zu den Lieferanten 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 Dienstleistungen Dritter ausgenutzt werden. Die Einrichtungen sollten daher die Gesamtqualität der Produkte und Cybersicherheitsverfahren ihrer Lieferanten und Diensteanbieter, einschließlich ihrer sicheren Entwicklungsprozesse, bewerten und berücksichtigen.

(44) Unter den Diensteanbietern spielen die Anbieter verwalteter Sicherheitsdienste (Managed Security Services Providers, MSSP) in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die Erkennung und Bewältigung von Sicherheitsvorfällen unterstützen. Allerdings sind auch die MSSP selbst das Ziel von Cyberangriffen und stellen durch ihre enge Einbindung in die Tätigkeiten der Betreiber ein besonderes Cybersicherheitsrisiko dar. Die Einrichtungen sollten daher bei der Wahl eines MSSP erhöhte Sorgfalt walten lassen.

(44a) Die zuständigen nationalen Behörden können im Rahmen ihrer Aufsichtsaufgaben auch Cybersicherheitsdienste für beispielsweise Sicherheitsprüfungen und Penetrationstests oder die Reaktion auf Sicherheitsvorfälle nutzen. Um Einrichtungen und zuständige nationale Behörden bei der Auswahl qualifizierter und vertrauenswürdiger Anbieter von Cybersicherheitsdiensten zu unterstützen, sollte die Kommission mit Unterstützung der Kooperationsgruppe und der ENISA die Möglichkeit prüfen, einen Auftrag für ein europäisches Systeme für die Cybersicherheitszertifizierung gemäß Artikel 48 der Verordnung (EU) 2019/881 zu erteilen.

(45) Die Einrichtungen sollten sich auch mit Cybersicherheitsrisiken befassen, die sich aus ihren Interaktionen und Beziehungen zu anderen interessierten Kreisen in einem weiter gefassten Ökosystem ergeben. Insbesondere sollten die 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 Einrichtungen letztere alle geeigneten Cybersicherheitsmaßnahmen ergreifen, wenn sie die Datenverarbeitungs- und -analysedienste Dritter in Anspruch nehmen.

(46) Um die Hauptrisiken für die Lieferkette weiter anzugehen und den Einrichtungen in den unter diese Richtlinie fallenden Sektoren dabei zu helfen, Cybersicherheitsrisiken in Bezug auf die Lieferkette und die Lieferanten angemessen zu beherrschen, sollte die Kooperationsgruppe, an der die einschlägigen nationalen Behörden beteiligt sind, in Zusammenarbeit mit der Kommission und der ENISA koordinierte sektorenbezogene Lieferketten-Risikobewertungen – wie im Fall der 5G-Netze gemäß der einschlägigen Empfehlung (EU) 2019/534[21] – durchführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.

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

(47) Bei den Lieferketten-Risikobewertungen 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 EU-weit koordinierten Risikobewertung zur Cybersicherheit in 5G-Netzen 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 gegen destabilisierende Ereignisse und v) die potenzielle künftige Bedeutung neuer IKT-Dienste, -Systeme oder -Produkte für die Tätigkeiten der Einrichtungen.

(48) Zur Straffung der rechtlichen Verpflichtungen, die Anbietern öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste sowie Vertrauensdiensteanbietern hinsichtlich der Sicherheit ihrer Netze und Informationssysteme auferlegt werden, und um diese Einrichtungen und ihre jeweiligen zuständigen Behörden von dem durch diese Richtlinie geschaffenen Rechtsrahmen profitieren zu lassen (u. a. Benennung der für die Bewältigung von Risiken und Vorfällen zuständigen Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs), Beteiligung der zuständigen Behörden und Stellen an der Arbeit der Kooperationsgruppe und des CSIRT-Netzwerks), sollten sie in den Anwendungsbereich dieser Richtlinie aufgenommen werden. Die entsprechenden Bestimmungen der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates[22] und der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates[23], mit denen diesen Arten von Einrichtungen Sicherheitsanforderungen und Meldepflichten auferlegt werden, sollten daher aufgehoben werden.

---

22 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).

23 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).

(48a) Die in dieser Richtlinie festgelegten Sicherheitspflichten sollten als Ergänzung zu den Anforderungen betrachtet werden, denen die Vertrauensdiensteanbietern gemäß der Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) 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 Sicherheits- und Meldepflichten sollten auch den physischen Schutz des angebotenen Dienstes betreffen. Artikel 24 der Verordnung (EU) Nr. 910/2014 sollte weiterhin gelten.

(48aa) Die Mitgliedstaaten können den eIDAS-Aufsichtsstellen 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 der eIDAS-Verordnung gewonnen wurden. Wird diese Funktion einer anderen Stelle übertragen, sollten die nach dieser Richtlinie zuständigen nationalen Behörden zeitnah und eng zusammenarbeiten, indem sie die einschlägigen Informationen austauschen, um eine wirksame Aufsicht und Einhaltung der Anforderungen dieser Richtlinie und der Verordnung [XXXX/XXXX] durch die Vertrauensdiensteanbieter zu gewährleisten.

Gegebenenfalls sollten die nach dieser Richtlinie zuständigen nationalen Behörden unverzüglich die eIDAS-Aufsichtsstellen über gemeldete erhebliche Cyberbedrohungen oder Vorfälle mit Auswirkungen auf Vertrauensdienste und die Nichteinhaltung der Anforderungen dieser 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 eIDAS-Aufsichtsstelle und die nach dieser Richtlinie zuständige Behörde zu erreichen. Die Vorschriften über die Meldepflichten sollten die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates[24] unberührt lassen.

---

[24] 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).

(49) Sofern angebracht und um unnötige Unterbrechungen zu vermeiden, sollten **die** bestehenden nationalen Leitlinien [...], die zur Umsetzung der Vorschriften über Sicherheitsmaßnahmen gemäß [...] **den Artikeln** 40 **und 41** [...] der Richtlinie (EU) 2018/1972 [...] erlassen wurden, [...] **bei den von den Mitgliedstaaten in Bezug auf die vorliegende Richtlinie festzulegenden Umsetzungsregelungen berücksichtigt werden, wobei auf den Erkenntnissen und Fähigkeiten aufzubauen ist, die im Zusammenhang mit Maßnahmen zum Sicherheitsrisikomanagement und der Meldung von Sicherheitsvorfällen bereits im Rahmen der Richtlinie (EU) 2018/1972 gewonnen wurden**. **Zudem kann die ENISA Leitlinien zu den Sicherheits- und Meldepflichten 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 übertragen, um die Fortführung der derzeitigen Verfahrensweisen sicherzustellen und auf den Erkenntnissen und Erfahrungen aufzubauen, die bei der Anwendung der Richtlinie (EU) 2018/1972 gewonnen wurden.**

(50) Angesichts der wachsenden Bedeutung nummernunabhängiger interpersoneller Kommunikationsdienste muss sichergestellt werden, dass auch für diese Dienste angemessene Sicherheitsanforderungen entsprechend ihrer spezifischen Art und wirtschaftlichen Bedeutung gelten. Die Anbieter solcher Dienste sollten daher auch ein Sicherheitsniveau von Netz- und Informationssystemen gewährleisten, das dem bestehenden Risiko angemessen ist. Da die Anbieter nummernunabhängiger interpersoneller Kommunikationsdienste üblicherweise keine tatsächliche Kontrolle über die Signalübertragung über Netze ausüben, kann das Risiko 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.

(51) Das Funktionieren des Internets ist für den Binnenmarkt wichtiger denn je. Die Dienstleistungen praktisch 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 für öffentliche elektronische Kommunikationsnetze, z. B. Internet-Backbone- oder Seekabel, geeignete Cybersicherheitsmaßnahmen bestehen und diesbezügliche Sicherheitsvorfälle gemeldet werden.

(52) Gegebenenfalls sollten die Einrichtungen die Empfänger ihrer Dienste über besondere [...] Bedrohungen sowie über Maßnahmen informieren, die sie ergreifen können, um das sich [...] **aus einer erheblichen Cyberbedrohung ergebende** Risiko für sich selbst zu mindern. **Die Einrichtungen sollten gegebenenfalls und insbesondere in Fällen, in denen die erhebliche Cyberbedrohung eintreten kann, neben den zuständigen Behörden oder den CSIRTs gleichzeitig auch die Empfänger ihrer Dienste über die Bedrohung selbst unterrichten.** Die Verpflichtung zur Information der Empfänger über solche Bedrohungen sollte die Einrichtungen nicht von der Pflicht befreien, auf eigene Kosten angemessene Sofortmaßnahmen zu ergreifen, um jedwede Cyberbedrohung zu verhüten oder zu beseitigen und das normale Sicherheitsniveau des Dienstes wiederherzustellen. Die Bereitstellung solcher Informationen über [...] **Cyberbedrohungen** sollte für die Empfänger kostenlos sein.

(53) Insbesondere sollten die Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste die Empfänger der Dienste über besondere und erhebliche Cyberbedrohungen sowie über Maßnahmen zum Schutz von Kommunikationsinhalten, die sie treffen können, informieren, z. B. den Einsatz spezieller Software oder von Verschlüsselungsverfahren.

(54) Zur Aufrechterhaltung der Sicherheit elektronischer Kommunikationsnetze und -dienste sollte die Verschlüsselung, insbesondere von Ende zu Ende, gefördert werden; erforderlichenfalls sollte sie für die Anbieter solcher Dienste und Netze im Einklang mit den Grundsätzen der Sicherheit und des Schutzes der Privatsphäre mittels datenschutzfreundlicher Voreinstellungen und Technikgestaltung für die Zwecke des Artikels 18 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 Ermittlung, Aufdeckung und Verfolgung von Straftaten im Einklang mit dem Unionsrecht zu ermöglichen, in Einklang gebracht werden. Lösungen für den rechtmäßigen Zugang zu Informationen in End-zu-End-verschlüsselter Kommunikation sollten die Wirksamkeit der Verschlüsselung beim Schutz der Privatsphäre und der Sicherheit der Kommunikation aufrechterhalten und zugleich eine wirksame Reaktion auf Straftaten gewährleisten.

(55) Mit dieser Richtlinie wird ein zweistufiger Ansatz für die Meldung von Sicherheitsvorfällen festgelegt, um die richtige Balance herzustellen zwischen einer zeitnahen Meldung einerseits, die einer potenziellen Ausbreitung von Sicherheitsvorfällen entgegenwirkt und den Einrichtungen die Möglichkeit gibt, Unterstützung zu erhalten, und einer detaillierten Meldung andererseits, bei der aus individuellen Sicherheitsvorfällen wichtige Lehren gezogen werden und einzelne Unternehmen und ganze Sektoren ihre Resilienz gegenüber Cyberbedrohungen im Laufe der Zeit verbessern können. Erhalten Einrichtungen Kenntnis von einem Sicherheitsvorfall, sollten sie innerhalb von 24 Stunden eine erste Meldung übermitteln und spätestens einen Monat danach einen Abschlussbericht vorlegen müssen. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständigen Behörden über den Sicherheitsvorfall zu unterrichten und es der Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. Gegebenenfalls sollte aus dieser Meldung hervorgehen, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der meldenden Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. Zur weiteren Verhinderung, dass die Meldepflichten für Sicherheitsvorfälle entweder zulasten der Ressourcen gehen, auf solche Vorfälle zu reagieren, oder entsprechende Anstrengungen der Einrichtungen anderweitig beeinträchtigt werden, sollten die Mitgliedstaaten auch vorsehen, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von der Frist von 24 Stunden für die Erstmeldung bzw. einem Monat für den Abschlussbericht abweichen kann.

(55a) Ein proaktiver Ansatz gegen Cyberbedrohungen ist ein wesentlicher Bestandteil des Cybersicherheitsrisikomanagements und sollte den zuständigen Behörden ermöglichen, wirksam zu verhindern, dass Cyberbedrohungen in tatsächliche Sicherheitsvorfälle münden, die erhebliche materielle oder immaterielle Verluste verursachen können. Zu diesem Zweck ist die Meldung erheblicher Cyberbedrohungen von zentraler Bedeutung.

(56) Wesentliche und wichtige Einrichtungen sind häufig in einer Situation, in der ein bestimmter Sicherheitsvorfall aufgrund seiner Merkmale und sich aus verschiedenen Rechtsinstrumenten ergebender Meldepflichten verschiedenen Behörden gemeldet werden muss. Solche Fälle führen zu zusätzlichen Belastungen und unter Umständen auch zu Unsicherheiten hinsichtlich des Formats solcher Meldungen und der für sie geltenden Verfahren. Vor diesem Hintergrund und zur Vereinfachung der Meldung von Sicherheitsvorfällen [...] **können** die Mitgliedstaaten eine *zentrale Anlaufstelle* für alle Meldungen einrichten, die aufgrund dieser Richtlinie sowie anderer EU-Rechtsvorschriften wie der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben sind. Die ENISA sollte in Zusammenarbeit mit der Kooperationsgruppe mittels Leitlinien einheitliche Meldemuster erstellen, die die im Unionsrecht geforderten Informationen vereinfachen und straffen und den Aufwand für die Unternehmen verringern würden.

(57) 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 das EC3 und die ENISA bei der Koordinierung zwischen den zuständigen Behörden und den Strafverfolgungsbehörden verschiedener Mitgliedstaaten wünschenswert.

(58) Häufig ist bei Sicherheitsvorfällen der Schutz personenbezogener Daten nicht mehr gewährleistet. In diesem Zusammenhang sollten die zuständigen Behörden gemäß der Richtlinie 2002/58/EG mit den Datenschutzbehörden und den Aufsichtsbehörden zusammenarbeiten und Informationen über alle relevanten Angelegenheiten austauschen.

(59) Die Pflege genauer und vollständiger Datenbanken mit Domänennamen und Registrierungsdaten (sogenannte „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 Union beiträgt. Werden auch personenbezogene Daten verarbeitet, so muss diese Verarbeitung mit dem EU-Datenschutzrecht im Einklang stehen.

(60) Die Verfügbarkeit und zeitnahe Zugänglichkeit dieser Daten für Behörden, einschließlich der nach Unionsrecht oder nationalem Recht für die Verhütung, Ermittlung oder Verfolgung von Straftaten zuständigen Behörden, CERTs, CSIRTs und – soweit es die Daten ihrer Kunden betrifft – Anbietern elektronischer Kommunikationsnetze und -dienste sowie Anbietern von Cybersicherheitstechnologien und -diensten, die im Namen dieser Kunden tätig sind, ist von wesentlicher Bedeutung, um Missbrauch des Domänennamensystems abzuwenden und zu bekämpfen und insbesondere Cybersicherheitsvorfällen vorzubeugen, sie zu erkennen und zu bewältigen. Dieser Zugang sollte, soweit personenbezogene Daten betroffen sind, mit dem EU-Datenschutzrecht im Einklang stehen.

(61) Zur Gewährleistung der Verfügbarkeit genauer und vollständiger Domänennamen-Registrierungsdaten sollten die TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen (sogenannte Registrierstellen), die Integrität und Verfügbarkeit von Domänennamen-Registrierungsdaten erfassen und garantieren. **Bei den Registrierungsdaten sollten die Einrichtungen insbesondere den Namen und die E-Mail-Adresse des Registrierenden überprüfen.** [...] **D**ie TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten Grundsätze und Verfahren festlegen, um im Einklang mit den EU-Datenschutzvorschriften genaue und vollständige Registrierungsdaten zu erfassen und zu pflegen sowie unrichtige Registrierungsdaten zu verhindern bzw. zu berichtigen.

(62) TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Domänennamen-Registrierungsdaten, die nicht den EU-Datenschutzvorschriften unterliegen, z. B. Daten, die juristische Personen betreffen, öffentlich zugänglich machen[25]. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, sollten es auch ermöglichen, dass berechtigte Zugangsnachfrager rechtmäßigen Zugang zu bestimmten Domänennamen-Registrierungsdaten natürlicher Personen im Einklang mit dem EU-Datenschutzrecht erhalten. Die Mitgliedstaaten sollten sicherstellen, dass TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, Anträge [...] auf Offenlegung von Domänennamen-Registrierungsdaten**, die von berechtigten Zugangsnachfragern – wie etwa nach Unionsrecht oder nationalem Recht für die nationale Sicherheit oder Strafgerichtsbarkeit zuständige Behörden oder CSIRTs – eingereicht wurden,** unverzüglich beantworten. TLD-Register und die Einrichtungen, die Domänennamen-Registrierungsdienste für sie erbringen, sollten Grundsätze und Verfahren für die Veröffentlichung und Offenlegung von Registrierungsdaten festlegen, einschließlich Leistungsvereinbarungen für die Bearbeitung von Anträgen berechtigter Zugangsnachfrager. Das Zugangsverfahren kann 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. **Die Mitgliedstaaten sollten sicherstellen, dass alle Arten des Zugangs zu (personenbezogene und nicht personenbezogenen) Domänenregistrierungsdaten kostenlos sind.** Zur Förderung einheitlicher Verfahren für den gesamten Binnenmarkt kann die Kommission unbeschadet der Zuständigkeiten des Europäischen Datenschutzausschusses **im Einklang mit den von der Multi-Stakeholder-Gemeinschaft entwickelten internationalen Normen und ergänzend dazu** Leitlinien zu solchen Verfahren erlassen.

---

25 Erwägungsgrund 14 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates: „Diese Verordnung gilt nicht für die Verarbeitung personenbezogener Daten juristischer Personen und insbesondere als juristische Person gegründeter Unternehmen, einschließlich Name, Rechtsform oder Kontaktdaten der juristischen Person."

(63) [...] **D**ie wesentlichen und wichtigen Einrichtungen, die unter diese Richtlinie fallen, sollten der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen. **Einrichtungen gemäß Anhang I Nummern 1 bis 7 und 10, Vertrauensdiensteanbieter und Betreiber von Internet-Knoten gemäß Anhang I Nummer 8 und Einrichtungen gemäß Anhang II Nummern 1 bis 5 sollten der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie niedergelassen sind.** [...] Falls die Einrichtung in mehreren Mitgliedstaaten Dienste erbringt **oder eine Niederlassung hat**, sollte sie unter die getrennte und parallele gerichtliche Zuständigkeit der betreffenden Mitgliedstaaten fallen. Die zuständigen Behörden dieser Mitgliedstaaten sollten zusammenarbeiten, einander Amtshilfe leisten und gegebenenfalls gemeinsame Aufsichtstätigkeiten durchführen. **Beschließen die Mitgliedstaaten, ihre gerichtlichen Zuständigkeit auszuüben, so sollten sie vermeiden, dass ein und dieselbe Handlung mehr als einmal wegen eines Verstoßes gegen die in dieser Richtlinie festgelegten Verpflichtungen sanktioniert wird.**

(64) Da die Dienste und Tätigkeiten, die von DNS-Diensteanbietern, TLD-Namenregistern, **Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen,** Betreibern von Inhaltszustellnetzen, Anbietern von Cloud-Computing-Diensten sowie Anbietern von Rechenzentrumsdiensten und Anbietern digitaler Dienste erbracht werden, grenzübergreifenden Charakter haben, sollte jeweils immer nur ein Mitgliedstaat für diese Einrichtungen zuständig sein. Die gerichtliche 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 der Ort 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 Unternehmen in der Union befindet. **Kann der Ort, an dem solche Entscheidungen vorwiegend getroffen werden, nicht bestimmt werden oder w**erden solche Entscheidungen nicht in der Union getroffen, sollte davon ausgegangen werden, 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.

(64a) Wenn ein Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste einen rekursiven DNS-Dienst nur als Teil des Internetzugangsdienstes anbietet, so sollte davon ausgegangen werden, dass die Einrichtung der gerichtlichen Zuständigkeit aller Mitgliedstaaten unterliegt, in denen sie ihre Dienste erbringt.

(64aa) Die ENISA sollte auf der Grundlage der Meldungen, die sie von den Mitgliedstaaten – gegebenenfalls über deren nationale Eigenmeldungsverfahren – erhalten hat, ein Register für Einrichtungen aufstellen und führen, um zu gewährleisten, dass es einen klaren Überblick über die DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, Betreiber von Inhaltszustellnetzen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten und Anbieter digitaler Dienste, die im Rahmen des Anwendungsbereichs dieser Richtlinie in der gesamten Union Dienste anbieten, gibt. Um die Richtigkeit und Vollständigkeit der in dieses Register aufzunehmenden Informationen sicherzustellen, sollten die Mitgliedstaaten der ENISA die in ihren 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.

(65) Bieten DNS-Diensteanbieter, TLD-Namenregister, Betreiber von Inhaltszustellnetzen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten oder Anbieter digitaler Dienste, die keine Niederlassung in der Union haben, Dienste in der Union an, so sollten sie einen Vertreter benennen. Um festzustellen, ob eine solche Einrichtung in der Union Dienste anbietet, sollte geprüft werden, ob sie offensichtlich 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 sind zur Feststellung einer solchen Absicht ebenso wenig ausreichend 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 anderen 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 die CSIRTs möglich sein, mit ihm Kontakt aufzunehmen. 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.

(66) Werden nach nationalem Recht oder Unionsrecht als Verschlusssache geltende Informationen gemäß den Bestimmungen dieser Richtlinie ausgetauscht, gemeldet oder auf andere Weise weitergegeben, so sollten die entsprechenden besonderen Vorschriften für den Umgang mit Verschlusssachen angewandt werden.

(67) Da Cyberbedrohungen komplexer und technisch ausgereifter werden, hängen gute Erkennungs- und 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 die Einrichtungen Bedrohungen abwehren können, bevor sie in reale Sicherheitsvorfälle münden, und in der Lage sind, die Auswirkungen von Sicherheitsvorfällen besser einzudämmen und effizienter zu reagieren. In Ermangelung von Leitlinien auf Unionsebene scheinen mehrere Faktoren einen solchen Wissensaustausch verhindert zu haben, insbesondere die nicht geklärte Vereinbarkeit mit den Wettbewerbs- und Haftungsvorschriften.

(68) Die Einrichtungen sollten ermutigt werden, ihre individuellen Kenntnisse und praktischen Erfahrungen auf strategischer, taktischer und operativer Ebene gemeinsam zu nutzen, damit sich ihre Fähigkeit verbessert, Cyberbedrohungen angemessen zu bewerten, zu überwachen, abzuwehren und auf sie zu reagieren. Daher muss dafür gesorgt werden, dass auf Unionsebene Mechanismen für Vereinbarungen über den freiwilligen Informationsaustausch entstehen können. Zu diesem Zweck sollten die Mitgliedstaaten auch einschlägige Einrichtungen, die nicht unter diese Richtlinie fallen, aktiv unterstützen und dazu anhalten, sich an solchen Mechanismen zum Informationsaustausch zu beteiligen. Diese Mechanismen sollten unter uneingeschränkter Einhaltung der Wettbewerbsvorschriften und des Datenschutzrechts der Union eingerichtet werden.

(69) Die Verarbeitung personenbezogener Daten durch **wesentliche und wichtige** Einrichtungen **und** [...] Anbieter von Sicherheitstechnologien und -diensten [...] **kann** im Sinne der Verordnung (EU) 2016/679 **als zur Erfüllung einer rechtlichen Verpflichtung erforderlich oder als im berechtigten Interesse des jeweiligen Verantwortlichen liegend erachtet werden**, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist. Dies **kann** [...] auch Folgendes einschließen: Maßnahmen im Hinblick auf die Verhütung, Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen, Maßnahmen zur Sensibilisierung für spezifische Cyberbedrohungen, Informationsaustausch im Zusammenhang mit der Behebung von Schwachstellen und ihrer koordinierten Offenlegung, freiwilliger Austausch von Informationen über solche Sicherheitsvorfälle sowie über Cyberbedrohungen und Schwachstellen, Gefährdungsindikatoren, Taktiken, Vorgehensweisen und Verfahren, Cybersicherheitswarnungen und Konfigurationstools. Diese Maßnahmen können die Verarbeitung [...] **verschiedener** Arten personenbezogener Daten erfordern [...]**, so zum Beispiel** IP-Adressen, Uniform Resource Locators (URL-Adressen), Domänennamen und E-Mail-Adressen. **Die Verarbeitung personenbezogener Daten durch die zuständigen Behörden, die Cybersicherheitsanlaufstellen und die CSIRTs sollte im nationalen Recht geregelt und im Sinne des Artikels 6 Absatz 1 Buchstaben c und e der Verordnung (EU) 2016/679 zur Erfüllung einer rechtlichen Verpflichtung oder für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, als erforderlich erachtet werden.**

(69a) Soweit dies für die Gewährleistung der Sicherheit der Netz- und Informationssysteme der wesentlichen und wichtigen Einrichtungen unbedingt notwendig und verhältnismäßig ist, können in den Rechtsvorschriften der Mitgliedstaaten Bestimmungen festgelegt werden, die es den zuständigen Behörden, den Cybersicherheitsanlaufstellen und den CSIRTs ermöglichen, besondere Kategorien personenbezogener Daten gemäß Artikel 9 der Verordnung (EU) 2016/679 zu verarbeiten, wobei insbesondere angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen natürlicher Personen vorgesehen werden, wozu auch technische Beschränkungen einer Weiterverwendung solcher Daten und modernste Sicherheits- und Datenschutzmaßnahmen wie Pseudonymisierung oder Verschlüsselung gehören, wenn der verfolgte Zweck durch eine Anonymisierung erheblich beeinträchtigt würde.

(70) 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 sowohl für die Einrichtungen als auch für die zuständigen Behörden ausgewogen zu gestalten. Wesentliche Einrichtungen sollten deshalb einem vollständigen Aufsichtssystem (ex-ante und ex-post) und wichtige Einrichtungen einem vereinfachten Aufsichtssystem (nur ex-post) unterliegen. Im letzteren Fall bedeutet dies, dass wichtige Einrichtungen die Erfüllung der Anforderungen an das Cybersicherheitsrisikomanagement nicht systematisch [...] dokumentieren [...] **müssten** und die zuständigen Behörden ein reaktives Ex-post-Aufsichtskonzept anwenden und 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 Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen 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.**

(70a) 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 Durchführung, Häufigkeit oder Art der Vor-Ort-Kontrollen oder gezielten Sicherheitsprüfungen oder Sicherheitsscans, Art der verlangten Informationen und Detaillierungsgrad dieser Informationen. Solche Aufsichtsmethoden können auch mit Arbeitsprogrammen einhergehen und regelmäßig bewertet und überprüft werden, auch in Bezug auf Aspekte wie Mittelzuweisung und -bedarf.

(70b) Bei Einrichtungen der öffentlichen Verwaltung sollten die Aufsichtsbefugnisse im Einklang mit den nationalen Rahmenbedingungen und der nationalen Rechtsordnung ausgeübt werden. Die Mitgliedstaaten sollten über die Einführung von angemessenen, verhältnismäßigen und wirksamen Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf diese Einrichtungen entscheiden können.

(70c) Um die Einhaltung bestimmter Risikomanagementmaßnahmen im Bereich der Cybersicherheit nachzuweisen, könnten die Mitgliedstaaten wesentliche und wichtige Einrichtungen dazu verpflichten, qualifizierte Vertrauensdienste oder notifizierte elektronische Identifizierungssysteme gemäß der Verordnung (EU) Nr. 910/2014 zu nutzen.

(71) Für eine wirksame Durchsetzung sollte ein Mindestumfang von Verwaltungssanktionen für Verstöße gegen die Verpflichtungen im Bereich des Cybersicherheitsrisikomanagements und die Meldepflichten gemäß dieser Richtlinie festgelegt werden, womit für die gesamte Union ein klarer und kohärenter Rahmen für solche Sanktionen geschaffen wird. Folgendem sollte gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, den tatsächlich entstandenen Schäden oder Verlusten bzw. den Schäden oder Verlusten, die hätten entstehen können, der Frage, ob der Verstoß vorsätzlich oder fahrlässig begangen wurde, den Maßnahmen zur Vermeidung oder Minderung der entstandenen Schäden/Verluste, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, dem Umfang der Zusammenarbeit mit der Aufsichtsbehörde sowie jedem anderen erschwerenden oder mildernden Umstand. Für die Verhängung von Sanktionen einschließlich Geldbußen sollte es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, entsprechen.

(71a) Die Bestimmungen über die Haftung natürlicher Personen mit bestimmten Verantwortlichkeiten innerhalb einer Einrichtung für einen Verstoß gegen ihre Pflicht, die Einhaltung der in dieser Richtlinie festgelegten Verpflichtungen sicherzustellen, verpflichten die Mitgliedstaaten nicht dazu, bei Schäden, die Dritten durch einen solchen Verstoß entstanden sind, für eine strafrechtliche Verfolgung sorgen oder die zivilrechtliche Haftung gewährleisten.

(72) 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.

(73) Werden Geldbußen Unternehmen auferlegt, sollte zu diesem Zweck der Begriff „Unternehmen“ im Sinne der Artikel 101 und 102 AEUV verstanden werden. Werden Geldbußen Personen auferlegt, bei denen es sich nicht um Unternehmen handelt, so sollte die Aufsichtsbehörde 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.

(74) Die Mitgliedstaaten **können** [...] strafrechtliche Sanktionen für Verstöße gegen die nationalen Vorschriften zur Umsetzung dieser Richtlinie festlegen [...]. 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 ausgelegt worden ist, führen.

(75) Soweit diese Richtlinie verwaltungsrechtliche Sanktionen nicht harmonisiert oder wenn es in anderen Fällen — beispielsweise bei schweren Verstößen gegen die Verpflichtungen aus dieser Richtlinie — erforderlich ist, sollten die Mitgliedstaaten eine Regelung anwenden, die wirksame, verhältnismäßige und abschreckende Sanktionen vorsieht. Im Recht der Mitgliedstaaten sollte geregelt werden, ob diese Sanktionen strafrechtlicher oder verwaltungsrechtlicher Art sind.

(76) Um die Wirksamkeit und Abschreckungskraft der Sanktionen bei Verstößen gegen die Verpflichtungen aus dieser Richtlinie zu erhöhen, sollten die zuständigen Behörden befugt sein, Sanktionen zu verhängen, die darin bestehen, die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste auszusetzen und natürlichen Personen die Ausübung von Leitungsaufgaben vorübergehend zu untersagen. Angesichts ihrer Schwere und ihrer Auswirkungen auf die Tätigkeiten der Einrichtungen und letztlich auf ihre Verbraucher sollten solche Sanktionen 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 erlittenen Schadens und/oder der erlittenen Verluste ergriffenen Maßnahmen. Solche Sanktionen sollten nur als äußerstes Mittel verhängt werden, also erst nachdem die anderen einschlägigen Durchsetzungsmaßnahmen nach dieser Richtlinie ausgeschöpft wurden, und nur so lange, bis die betroffenen Einrichtungen die erforderlichen Maßnahmen zur Behebung der Mängel ergreifen oder die Anforderungen der zuständigen Behörde, auf die sich die Sanktionen beziehen, erfüllen. Für die Verhängung solcher Sanktionen muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta der Grundrechte der Europäischen Union, einschließlich des Rechts auf wirksamen Rechtsschutz und ein faires Verfahren, der Unschuldsvermutung und des Rechts auf Verteidigung, entsprechen.

(76a) Um eine wirksame Aufsicht und Durchsetzung insbesondere in grenzüberschreitenden Fällen zu gewährleisten, sollten die Mitgliedstaaten, bei denen ein Amtshilfeersuchen eingegangen ist, in einem dem Ersuchen entsprechenden Umfang geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die betreffende Einrichtung, die in ihrem Hoheitsgebiet Dienste anbietet oder ein Netz- und Informationssystem betreibt, ergreifen.

(77) 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 im Zusammenhang mit personenbezogenen Daten vorzugehen.

(78) Die Richtlinie sollte darauf abzielen, auf Ebene der Organisationen ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Meldepflichten im Bereich der Cybersicherheit sicherzustellen. Aus diesen Gründen sollten die Verwaltungsorgane der unter diese Richtlinie fallenden Einrichtungen die Cybersicherheitsrisikomaßnahmen genehmigen und deren Umsetzung überwachen.

(79) Es sollte ein Peer-**Learning-System** [...] eingeführt werden, **das dazu beiträgt, das gegenseitige Vertrauen zu stärken und aus bewährten Verfahren und Erfahrungen zu lernen, und das einen fachlichen Austausch zwischen** [...] von den Mitgliedstaaten benannten Sachverständigen **über** die Umsetzung der Cybersicherheitsstrategien [...] **ermöglicht**. **Bei der Umsetzung des Peer-Learning-Systems sollte besonders darauf geachtet werden, dass es nicht mit unnötiger und unverhältnismäßiger Belastung für die zuständigen Behörden der Mitgliedstaaten einhergeht. Die Kommission sollte alle Möglichkeiten prüfen, wie die finanzielle Deckung der möglichen Kosten für die Organisation von Peer-Learning-Missionen garantiert werden könnte. Darüber hinaus sollte im Zusammenhang mit dem Peer-Learning-System den Ergebnissen ähnlicher Mechanismen, wie dem Peer-Review-System des CSIRT-Netzwerks, Rechnung getragen, ein Mehrwert geschaffen und Doppelarbeit vermieden werden. Die Umsetzung des Peer-Learning-Systems sollte die Rechtsvorschriften der Mitgliedstaaten und der Union über den Schutz vertraulicher oder als Verschlusssachen eingestufter Informationen unberührt lassen. Vor Beginn der Peer-Learning-Runden können die Mitgliedstaaten eine Eigenbewertung der relevanten Aspekte durchführen. Auf Ersuchen der Kooperationsgruppe kann die ENISA bei Bedarf Orientierungshilfen für die Selbstbewertung und einschlägige Vorlagen bereitstellen. Die Mitgliedstaaten können beschließen, die sie jeweils betreffenden Berichte zu veröffentlichen.**

(80) [...]

(81) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung der einschlägigen Bestimmungen dieser Richtlinie in Bezug auf die Verfahrensmodalitäten, die für das Funktionieren der Kooperationsgruppe erforderlich sind, die technischen Elemente im Zusammenhang mit Risikomanagementmaßnahmen oder die Art der Informationen, das Format und das Verfahren für die Meldung von Sicherheitsvorfällen **sowie die Kategorien von Einrichtungen, die bestimmte zertifizierte IKT-Produkte, -Dienste und -Prozesse nutzen müssen**, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden.[26]

(82) Die Kommission sollte diese Richtlinie regelmäßig in Abstimmung mit interessierten Kreisen überprüfen, insbesondere um festzustellen, ob sie veränderten gesellschaftlichen, politischen oder technischen Bedingungen oder veränderten Marktbedingungen anzupassen ist.

---

26 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).

(83) Da das Ziel dieser Richtlinie, nämlich die Erreichung eines hohen gemeinsamen Cybersicherheitsniveaus in der 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.

(84) Diese Richtlinie steht mit den in der Charta der Grundrechte der Europäischen Union anerkannten Grundrechten und Grundsätzen, insbesondere der Achtung des Privatlebens und der Kommunikation, dem Schutz personenbezogener Daten, der unternehmerischen Freiheit, dem Eigentumsrecht, dem Recht auf einen wirksamen Rechtsbehelf und dem Recht, gehört zu werden, im Einklang. Diese Richtlinie sollte im Einklang mit diesen Rechten und Grundsätzen umgesetzt werden —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

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

(2) Zu diesem Zweck sieht diese Richtlinie Folgendes vor:

a) die Pflicht für alle Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden und zuständige nationale Behörden, zentrale Anlaufstellen und Reaktionsteams für IT-Sicherheitsvorfälle (Computer Security Incident Response Teams, CSIRTs) zu benennen;

b) Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Meldepflichten für Einrichtungen der in **den Anhängen I und II** aufgeführten Arten [...];

c) **Vorschriften und Pflichten** zum Austausch von Cybersicherheitsinformationen.

Artikel 2

Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche und private Einrichtungen der in **den Anhängen I und II** aufgeführten Arten**, die die Schwellenwerte für mittlere Unternehmen** im Sinne der Empfehlung 2003/361/EG der Kommission[27] **erreichen oder überschreiten**. **Artikel 3 Absatz 4 und Artikel 6 Absatz 2 Unterabsätze 2 und 3 des Anhangs der genannten Empfehlung gelten nicht für die Zwecke dieser Richtlinie.**

(2) Unabhängig von der Größe der Einrichtungen **gemäß Absatz 1** gilt diese Richtlinie [...] auch [...], wenn [...]

a) die Dienste von einer der folgenden Einrichtungen erbracht werden:

(i) **Anbietern** öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste gemäß Anhang I Nummer 8;

(ii) **qualifizierten Vertrauensdiensteanbietern gemäß Anhang I Nummer XX;**

iii) **nichtqualifizierten Vertrauensdiensteanbietern gemäß Anhang I Nummer XX;**

iv) Namenregistern der Domäne oberster Stufe [...] gemäß Anhang I Nummer 8;

b) [...]

---

27 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).

c) 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**;

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

e) eine mögliche Störung des von der Einrichtung erbrachten Dienstes zu **wesentlichen** Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

f) [...];

g) wenn die Einrichtung als kritische Einrichtung im Sinne der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates[28] [Richtlinie über die Resilienz kritischer Einrichtungen] **[**oder als einer kritischen Einrichtung gleichgestellte Einrichtung gemäß Artikel 7 der genannten Richtlinie**]** gilt.

(2a) Diese Richtlinie gilt unabhängig von deren Größe auch für Einrichtungen der öffentlichen Verwaltung von Zentralregierungen, die in einem Mitgliedstaat nach nationalem Recht als solche anerkannt sind und auf die in Anhang I Nummer 9 Bezug genommen wird. Die Mitgliedstaaten können festlegen, dass diese Richtlinie auch für Einrichtungen der öffentlichen Verwaltung auf regionaler und lokaler Ebene gilt.

28 [vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt].

(3) [...]

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

(3a) 1. Diese Richtlinie gilt nicht für

a) Einrichtungen, die nicht in den Anwendungsbereich des Unionsrechts fallen, und unbeschadet des Absatzes 2 in jedem Fall alle Einrichtungen, die in erster Linie Tätigkeiten in den Bereichen Verteidigung, nationale Sicherheit, öffentliche Sicherheit oder Strafverfolgung ausüben, unabhängig davon, welche Einrichtung diese Tätigkeiten ausübt und ob es sich um eine öffentliche oder eine private Einrichtung handelt;

b) Einrichtungen, die Tätigkeiten in den Bereichen der Justiz, der Parlamente oder der Zentralbanken ausüben.

2. Wenn Einrichtungen der öffentlichen Verwaltung Tätigkeiten in diesen Bereichen nur im Rahmen ihrer Gesamttätigkeit ausüben, sind sie in vollem Umfang vom Anwendungsbereich dieser Richtlinie ausgenommen.

(3aa) Diese Richtlinie gilt nicht für

i) Tätigkeiten von Einrichtungen, die nicht in den Anwendungsbereich des Unionsrechts fallen, und in jedem Fall alle Tätigkeiten, die die nationale Sicherheit oder Verteidigung betreffen, unabhängig davon, welche Einrichtung diese Tätigkeiten ausübt und ob es sich um eine öffentliche oder eine private Einrichtung handelt;

ii) Tätigkeiten von Einrichtungen der Justiz, der Parlamente, Zentralbanken und im Bereich der öffentlichen Sicherheit, einschließlich Einrichtungen der öffentlichen Verwaltung, die zur Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung Tätigkeiten im Bereich der Strafverfolgung ausüben.

(3aaa) 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 zuwiderläuft.

(3aaaa) Das Unionsrecht betreffend den Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 und die Richtlinie 2002/58/EG, bleibt von dieser Richtlinie unberührt.

(3b) Diese Richtlinie gilt nicht für Einrichtungen, die gemäß Artikel 2 Absatz 4 der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung] von der DORA-Verordnung ausgenommen sind.

(4) Diese Richtlinie gilt unbeschadet [...][29] der Richtlinien 2011/93/EU[30] und 2013/40/EU[31] des Europäischen Parlaments und des Rates.

(5) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union und 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 wesentlicher oder wichtiger Einrichtungen geschützt.

---

29 [...]

30 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).

31 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).

Artikel 2a

Wesentliche und wichtige Einrichtungen

(1) Von den Einrichtungen, auf die diese Richtlinie Anwendung findet, gelten folgende als wesentlich:

i) Einrichtungen der in Anhang I Nummern 1 bis 8a und 10 dieser Richtlinie genannten Art, die die in der Empfehlung 2003/361/EG der Kommission festgelegten Schwellenwerte für mittlere Unternehmen überschreiten;

ii) mittlere Einrichtungen im Sinne von Artikel 2 Absatz 2 Buchstabe a Ziffer i;

iii) Einrichtungen im Sinne von Artikel 2 Absatz 2 Buchstabe a Ziffern ii und iv dieser Richtlinie, unabhängig von der Größe;

iv) Unternehmen im Sinne von Artikel 2 Absatz 2 Buchstabe g und Artikel 2 Absatz 2a dieser Richtlinie, unabhängig von der Größe;

v) Einrichtungen, die von den Mitgliedstaaten vor Inkrafttreten dieser Richtlinie nach der Richtlinie (EU) 2016/1148 oder nach nationalem Recht als Betreiber wesentlicher Dienste eingestuft wurden, sofern sie von den Mitgliedstaaten eingerichtet wurden;

vi) von Mitgliedstaaten anhand der Kriterien im Sinne von Artikel 2 Absatz 2 Buchstaben c bis e als wesentlich eingestufte Einrichtungen der in Anhang II genannten Art, die die in der Empfehlung 2003/361/EG der Kommission festgelegten Schwellenwerte für mittlere Unternehmen überschreiten;

vii) mittlere Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission, die von Mitgliedstaaten anhand der Kriterien im Sinne von Artikel 2 Absatz 2 Buchstaben c bis e als wesentlich eingestuft werden;

viii) Kleinstunternehmen oder kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission, die in Absatz 2 Buchstabe a Ziffer i genannt werden oder als Einrichtungen gemäß Artikel 2 Absatz 2 Buchstaben c bis e ermittelt wurden, die Mitgliedstaaten aufgrund nationaler Risikobewertungen als wesentlich einstufen.

(2) Von den Einrichtungen, auf die diese Richtlinie Anwendung findet, gelten folgende als wichtig:

i) Einrichtungen einer in Anhang I dieser Richtlinie genannten Art, die als mittlere Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission eingestuft werden, und Einrichtungen der in Anhang II genannten Art, die die Schwellenwerte für mittlere Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission[32] erreichen oder überschreiten;

ii) Einrichtungen im Sinne von Artikel 2 Absatz 2 Buchstabe a Ziffer iii dieser Richtlinie, unabhängig von der Größe;

iii) kleine und Kleinsteinrichtungen im Sinne von Artikel 2 Absatz 2 Buchstabe a Ziffer i;

iv) kleine und Kleinstunternehmen, die von den Mitgliedstaaten auf der Grundlage von Artikel 2 Absatz 2 Buchstaben c bis e als wichtige Einrichtungen eingestuft werden.

---

32 **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).**

Artikel 2a

Meldeverfahren

(1) Die Mitgliedstaaten können nationale Eigenmeldungsverfahren einrichten, in deren Rahmen alle unter diese Richtlinie fallenden Einrichtungen verpflichtet sind, den gemäß dieser Richtlinie zuständigen Behörden oder den dafür von den Mitgliedstaaten benannten Stellen zumindest ihren Namen, ihre Anschrift, Kontaktdaten, die Branche, in der sie tätig sind, oder die Art der Dienstleistung, die sie erbringen, sowie gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie unter diese Richtlinie fallende Dienstleistungen erbringen, zu übermitteln.

(2) Die Mitgliedstaaten übermitteln der Kommission bis zum [12 Monate nach Ablauf der Umsetzungsfrist dieser Richtlinie] in Bezug auf die Einrichtungen, die sie gemäß Artikel 2 Absatz 2 Buchstaben b bis e ermittelt haben, mindestens einschlägige Informationen zu der Zahl der ermittelten Einrichtungen, der Branche, zu der sie gehören, oder der Art der Dienstleistung(en), die sie im Sinne der Anhänge erbringen, und geben die jeweilige(n) Bestimmung(en) von Artikel 2 Absatz 2 an, auf deren Grundlage sie ermittelt wurden. Die Mitgliedstaaten überprüfen diese Liste regelmäßig und mindestens alle zwei Jahre und aktualisieren sie gegebenenfalls.

Artikel 2b

Sektorspezifische Rechtsakte der Union

(1) Wenn wesentliche oder wichtige Einrichtungen gemäß [...] sektorspezifischen Rechtsakten der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder **erhebliche** Sicherheitsvorfälle **oder** Cyberbedrohungen 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 VI,** keine Anwendung **auf solche Einrichtungen**. **Wenn die sektorspezifischen Rechtsakte der Union nicht für alle in den Anwendungsbereich dieser Richtlinie fallenden Unternehmen einer bestimmten Branche gelten, kommen die einschlägigen Bestimmungen dieser Richtlinie weiterhin im Falle der Unternehmen zur Anwendung, die nicht unter diese sektorspezifischen Bestimmungen fallen.**

(2) Die Anforderungen gemäß Absatz 1 dieses Artikels gelten als den in dieser Richtlinie festgelegten Verpflichtungen in ihrer Wirkung gleichwertig, wenn im betreffenden sektorspezifischen Rechtsakt der Union vorgesehen ist, dass die gemäß dieser Richtlinie zuständigen Behörden oder die benannten CSIRTs unverzüglichen, gegebenenfalls automatischen und direkten Zugang zu den Meldungen von Sicherheitsvorfällen haben und wenn

a) die Maßnahmen zum Cybersicherheitsrisikomanagement den in Artikel 18 Absätze 1 und 2 dieser Richtlinie festgelegten Maßnahmen in ihrer Wirkung mindestens gleichwertig sind oder

b) die Anforderungen bezüglich der Meldung erheblicher Sicherheitsvorfälle den Pflichten gemäß Artikel 20 Absätze 1 bis 6 in ihrer Wirkung mindestens gleichwertig sind.

(3) Die Kommission überprüft regelmäßig, dass die im Hinblick auf die gleichwertige Wirkung gemäß den Absätzen 1 und 2 dieses Artikels für sektorspezifische Rechtsakte der Union geltenden Anforderungen zur Anwendung kommen. Bei der Vorbereitung dieser regelmäßigen Überprüfungen konsultiert die Kommission die Kooperationsgruppe und die ENISA.

Artikel 3

Mindestharmonisierung

Unbeschadet ihrer sonstigen unionsrechtlichen Verpflichtungen können die Mitgliedstaaten [...] Bestimmungen erlassen oder beibehalten, die **in den unter diese Richtlinie fallenden Bereichen** ein höheres Cybersicherheitsniveau gewährleisten.

Artikel 4

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 2018/1972/EU,

   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**;

2a. „elektronische Kommunikationsdienste“ elektronische Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972;

3. „Cybersicherheit“ die Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[33];

4. „nationale Cybersicherheitsstrategie“ einen kohärenten **Steuerungsrahmen** eines Mitgliedstaats **zur Verwirklichung** strategischer Ziele und Prioritäten **im Bereich Cybericherheit** in diesem Mitgliedstaat;

5. „Sicherheitsvorfall“ jedes 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;

5a. „großer Cybersicherheitsvorfall“ einen Sicherheitsvorfall, der erhebliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat oder dessen Störungsausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt;

---

33 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).

6. „Bewältigung von Sicherheitsvorfällen“ alle Maßnahmen und Verfahren zur Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen sowie die Reaktion darauf;

6a. „Risiko“ aufgrund eines Sicherheitsvorfalls drohende Verluste oder Störungen, ausgedrückt als Kombination aus dem Ausmaß des Verlusts oder der Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls;

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

7a. **„erhebliche Cyberbedrohung“ eine Cyberbedrohung, die die Netz- und Informationssysteme einer Einrichtung oder ihrer Nutzer aufgrund ihrer technischen Merkmale mutmaßlich erheblich beeinträchtigen könnte, indem sie erhebliche materielle oder immaterielle Verluste verursacht;**

8. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion einer **IKT-Anlage oder** eines Systems [...], die bei einer Cyberbedrohung ausgenutzt werden kann;

8a. „Beinahe-Vorfall“ ein Ereignis, das die Netz- und Informationssysteme einer Einrichtung oder ihrer Nutzer hätte beschädigen können, dessen volle Wirkung aber erfolgreich verhindert wurde;

9. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag i) eines DNS-Diensteanbieters, eines TLD-Registers, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen gemäß Anhang I Nummer 8 oder im Auftrag ii) von in Anhang II Nummer 6 aufgeführten nicht in der Union niedergelassenen Einrichtungen 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;

10. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates[34];

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

12. „Internet-Knoten“ (Internet Exchange Point, IXP) eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr; ein IXP dient nur der Zusammenschaltung autonomer Systeme; ein IXP setzt nicht voraus, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; auch wird der betreffende Datenverkehr weder verändert noch anderweitig beeinträchtigt;

13. „Domänennamensystem (DNS)“ ein verteiltes hierarchisches Verzeichnissystem, das es den Endnutzern ermöglicht, Dienste und Ressourcen im Internet zu erreichen;

14. „DNS-Diensteanbieter“ eine Einrichtung, die [...] rekursive oder autoritative Dienste zur Auflösung von Domänennamen **zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern,** anbietet;

---

34 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).

15. „Namenregister der Domäne oberster Stufe“ (TLD-Register) 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**, außer in Fällen, in denen TLD-Namen von einem Register lediglich zum eigenen Gebrauch verwendet werden**;

15a. „Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen“ TLD-Namenregister, Registrierstellen für die TLDs und Agenten von Registrierstellen wie Wiederverkäufer und Anbieter von Proxy-Diensten;

16. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates[35];

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

[35] 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).

16b. „qualifizierter Vertrauensdiensteanbieter“ einen qualifizierten Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;

17. „Online-Marktplatz“ einen digitalen Dienst im Sinne des Artikels 2 Buchstabe n der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates[36];

18. „Online-Suchmaschine“ einen digitalen Dienst im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates[37];

19. „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 auf mehrere Standorte verteilt sind**;

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

---

36 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).

37 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).

21. „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;

22. „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;

23. „Einrichtung der öffentlichen Verwaltung“ eine **als solche in einem Mitgliedstaat nach nationalem Recht anerkannte** Einrichtung in [...], 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, einer Gebietskörperschaft oder von anderen Körperschaften des öffentlichen Rechts finanziert, oder sie untersteht hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften, oder sie 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.

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

25. „wesentliche Einrichtung“ jede Einrichtung **einer** in Anhang I **genannten Art, die gemäß Artikel 2a Absatz 1 als „wesentlich“ eingestuft wird**;

26. „wichtige Einrichtung“ jede Einrichtung **einer in den Anhängen I und II genannten Art, die gemäß Artikel 2a Absatz 2 als „wichtig“ eingestuft wird;**

26a. „IKT-Produkt“ ein IKT-Produkt im Sinne des Artikels 2 Nummer 12 der Verordnung (EU) 2019/881;

26aa. „IKT-Dienst“ einen IKT-Dienst im Sinne von Artikel 2 Nummer 13 der Verordnung (EU) 2019/881;

26ab. „IKT-Prozess“ einen IKT-Prozess im Sinne von Artikel 2 Nummer 14 der Verordnung (EU) 2019/881;

26ac. „Anbieter verwalteter Dienste“ jede Einrichtung, die durch laufende und regelmäßige Management-, Support- und aktive Verwaltungstätigkeiten in den Räumlichkeiten von Kunden, im eigenen Datenzentrum des Anbieters verwalteter Dienste (Hosting) oder im Datenzentrum Dritter Dienste wie Netzwerk-, Anwendungs-, Infrastruktur- und Sicherheitsdienste erbringt.

26ad. „Anbieter verwalteter Sicherheitsdienste“ eine Einrichtung, die ausgelagerte Überwachungs- und Managementdienste für Sicherheitseinheiten und -systeme anbietet. Zu diesen Diensten gehören in der Regel Managed-Firewall-Dienste, Angriffserkennung, VPN-Dienste, Überprüfung auf Schwachstellen und Antivirendienste.

Sie umfassen auch die Nutzung hochverfügbarer Sicherheitseinsatzzentren (entweder über die eigenen Anlagen oder über andere Anbieter von Datenzentren), die rund um die Uhr Dienste anbieten, damit Unternehmen das zur Aufrechterhaltung einer vertretbaren Sicherheitslage einzustellende, zu schulende und auf Dauer zu beschäftigende Sicherheitspersonal reduzieren können.

KAPITEL II

Koordinierte Rechtsrahmen für die Cybersicherheit

Artikel 5

Nationale Cybersicherheitsstrategie

(1) Jeder Mitgliedstaat verabschiedet eine nationale Cybersicherheitsstrategie, in der die strategischen Ziele sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus festgelegt werden. Die nationale Cybersicherheitsstrategie muss insbesondere Folgendes umfassen:

a) **die** für die Cybersicherheitsstrategie des jeweiligen Mitgliedstaats festgelegten Ziele und Prioritäten;

b) einen Steuerungsrahmen zur Verwirklichung dieser Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte sowie die Aufgaben und Zuständigkeiten der verschiedenen Behörden und [...] Akteure umfasst, die an der Umsetzung der Strategie beteiligt sind;

c) **Leitlinien** zur Ermittlung von relevanten Anlagen und **zur Bewertung von** Cybersicherheitsrisiken in diesem Mitgliedstaat;

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

e) [...]

f) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den zuständigen Behörden im Rahmen dieser Richtlinie und der Richtlinie (EU) XXXX/XXXX des Europäischen Parlaments und des Rates[38] [Richtlinie über die Resilienz kritischer Einrichtungen] für die Zwecke des Informationsaustauschs über **Cybersicherheitsrisiken,** Cyberbedrohungen **und Sicherheitsvorfälle sowie gegebenenfalls** der Wahrnehmung von Aufsichtsaufgaben**;**

fa) einen politischer Rahmen für die Koordinierung und die Zusammenarbeit zwischen den gemäß dieser Richtlinie zuständigen Behörden und den nach den sektorspezifischen Rechtsvorschriften benannten zuständigen Behörden.

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

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

b) **ein Konzept** für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und -Dienste bei der Vergabe öffentlicher Aufträge**, einschließlich Zertifizierung der Cybersicherheit**;

c) ein Konzept **für das Management von Schwachstellen, das die** Förderung und Erleichterung **einer freiwilligen** koordinierten Offenlegung von Schwachstellen im Sinne des Artikels 6 **Absatz 1 umfasst**;

d) ein Konzept im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit**,** Integrität **und Vertraulichkeit** des öffentlichen Kerns des offenen Internets;

e) ein Konzept zur Förderung und Entwicklung von **Aus- und Weiterbildung,** Kompetenzen, Sensibilisierungsmaßnahmen sowie Forschungs- und Entwicklungsinitiativen **im Bereich Cybersicherheit**;

---

38 *[vollständigen Titel und Fundstelle im Amtsblatt einfügen, sobald bekannt]*.

f) ein Konzept zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;

g) ein Konzept, einschlägige Verfahren und geeignete Instrumente für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheits-Informationen zwischen Unternehmen im Einklang mit dem Unionsrecht zu unterstützen;

h) ein Konzept, das auf die spezifischen Bedürfnisse von KMU – insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU – ausgerichtet ist und Orientierungshilfen sowie Unterstützung bei der Verbesserung ihrer Resilienz gegenüber **Cyberbedrohungen** bietet.

(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrer Verabschiedung. Die Mitgliedstaaten können **die Elemente der Strategie** von der Notifizierung ausnehmen, **die die** nationale Sicherheit **betreffen**.

(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien **regelmäßig,** mindestens **aber** alle **fünf** Jahre auf der Grundlage wesentlicher Leistungsindikatoren und ändern diese erforderlichenfalls. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) unterstützt die Mitgliedstaaten auf **deren** Anfrage bei der Entwicklung einer nationalen Strategie und wesentlicher Leistungsindikatoren für die Bewertung der Strategie.

Artikel 6

Koordinierte Offenlegung von Schwachstellen und europäisches Schwachstellenregister

(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs gemäß Artikel 9 als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der meldenden Einrichtung**, dem für die potenzielle Schwachstelle Verantwortlichen** und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten. **Jede natürliche oder juristische Person kann dem benannten CSIRT – auch anonym – Schwachstellen im Sinne von Artikel 4 Absatz 8 melden. Das benannte CSIRT sorgt für die sorgfältige Weiterverfolgung der Meldung und die Vertraulichkeit der Identität desjenigen, der die Schwachstelle meldet. Wenn** die gemeldete Schwachstelle **erhebliche Auswirkungen auf Einrichtungen in** mehreren **Mitgliedstaaten haben könnte,** arbeitet das benannte CSIRT jedes betroffenen Mitgliedstaats **gegebenenfalls** mit **den anderen benannten CSIRTs des** CSIRT-Netzwerks zusammen.

(2) Die ENISA entwickelt und pflegt **in Absprache mit der Kooperationsgruppe** ein europäisches Schwachstellenregister Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein und pflegt diese, damit insbesondere wichtige und wesentliche Einrichtungen sowie deren Anbieter von Netz- und Informationssystemen **freiwillig öffentlich bekannte** Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können und allen interessierten Kreisen Zugang zu den im Register enthaltenen Informationen über Schwachstellen gewährt werden kann. Das Register muss insbesondere Folgendes umfassen: Informationen zur Beschreibung der Schwachstelle, des betroffenen IKT-Produkts oder der betroffenen IKT-Dienste sowie zum Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann, Informationen zur Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches **von zuständigen nationalen Behörden oder CSIRTs herausgegebene** Orientierungshilfen für die Nutzer gefährdeter Produkte und Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können. **Die ENISA stellt sicher, dass das europäische Schwachstellenregister über eine sichere und belastbare Kommunikations- und Informationsinfrastruktur verfügt.**

Artikel 7

Nationale Rahmen für das Cybersicherheitskrisenmanagement

(1) Jeder Mitgliedstaat benennt eine oder mehrere für das Management **großer Cybersicherheitsvorfälle und -krisen** zuständige Behörden. Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient erfüllen zu können. **Sie gewährleisten die Kohärenz mit den geltenden Rahmen für das allgemeine Krisenmanagement.**

(2) Jeder Mitgliedstaat ermittelt die Kapazitäten, Mittel und Verfahren, die im Krisenfall für die Zwecke dieser Richtlinie eingesetzt werden können.

(3) Jeder Mitgliedstaat verabschiedet einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle und -krisen, in dem die Ziele und Modalitäten für das Management massiver Cybersicherheitsvorfälle 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 nationalen zuständigen Behörden;

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

d) die Vorsorgemaßnahmen, einschließlich **regelmäßiger** Übungen und Ausbildungsmaßnahmen;

e) die einschlägigen öffentlichen und privaten [...] Kreise sowie die beteiligten Infrastrukturen;

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 massiver Cybersicherheitsvorfälle und -krisen auf Unionsebene beteiligen und dieses unterstützen kann.

(4) Die Mitgliedstaaten **informieren** die Kommission **über die Benennung ihrer** zuständigen Behörden **gemäß Absatz 1** und übermitteln **die im Zusammenhang mit den Anforderungen gemäß Absatz 3 dieses Artikels relevanten Informationen über** ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle und -krisen [...] innerhalb von drei Monaten nach **dieser Benennung und** der Verabschiedung dieser Pläne. Die Mitgliedstaaten können bestimmte Informationen [...] ausnehmen, wenn und soweit dies für ihre nationale Sicherheit**, die öffentliche Sicherheit oder die Verteidigung** erforderlich ist.

Artikel 8

Nationale zuständige Behörden und zentrale Anlaufstellen

(1) Jeder Mitgliedstaat benennt eine oder mehrere für die Cybersicherheit und die in Kapitel VI dieser Richtlinie genannten Aufsichtsaufgaben zuständige Behörden. Die Mitgliedstaaten können dafür eine oder mehrere bereits bestehende Behörden benennen.

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

(3) Jeder Mitgliedstaat benennt eine für die Cybersicherheit zuständige nationale zentrale Anlaufstelle (im Folgenden „zentrale Anlaufstelle“). Benennt ein Mitgliedstaat nur eine zuständige Behörde, 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 in anderen Mitgliedstaaten sowie die sektorübergreifende Zusammenarbeit mit anderen nationalen zuständigen Behörden innerhalb des Mitgliedstaats zu gewährleisten.

(5) Die Mitgliedstaaten gewährleisten, dass die zuständigen Behörden gemäß Absatz 1 und die zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient erfüllen können und die Ziele dieser Richtlinie somit erreicht werden können. Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit der benannten Vertreter in der Kooperationsgruppe gemäß Artikel 12 sicher.

(6) Die Mitgliedstaaten notifizieren der Kommission unverzüglich die Benennung der zuständigen Behörde gemäß Absatz 1 und der zentralen Anlaufstelle gemäß Absatz 3, deren Aufgaben sowie etwaige spätere Änderungen dieser Angaben. Jeder Mitgliedstaat gibt seine Benennungen öffentlich bekannt. Die Kommission veröffentlicht die Liste der benannten zentralen Anlaufstellen.

Artikel 9

Reaktionsteams für IT-Sicherheitsvorfälle (CSIRTs)

(1) Jeder Mitgliedstaat benennt ein oder mehrere CSIRTs, die die in Artikel 10 Absatz 1 festgelegten Anforderungen erfüllen, mindestens die in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen abdecken und für die Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf zuständig sind. Ein CSIRT kann innerhalb einer zuständigen Behörde gemäß Artikel 8 eingerichtet werden.

(2) Die Mitgliedstaaten gewährleisten, dass jedes CSIRT mit angemessenen Ressourcen ausgestattet ist, damit es seine in Artikel 10 Absatz 2 aufgeführten Aufgaben wirksam erfüllen kann. **Bei der Wahrnehmung dieser Aufgaben können die CSIRTs die Erbringung bestimmter Dienstleistungen für Unternehmen auf der Grundlage eines risikobasierten Ansatzes vorrangig behandeln.**

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

(4) Die CSIRTs arbeiten mit vertrauenswürdigen sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen zusammen und tauschen mit diesen gemäß Artikel 26 gegebenenfalls einschlägige Informationen aus.

(5) Die CSIRTs nehmen am gemäß Artikel 16 organisierten **Peer-Learning** teil.

(6) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs in dem in Artikel 13 genannten CSIRT-Netzwerk wirksam, effizient und sicher zusammenarbeiten.

(7) Die Mitgliedstaaten teilen der Kommission unverzüglich die gemäß Absatz 1 benannten CSIRTs, das gemäß Artikel 6 Absatz 1 als Koordinator benannte CSIRT und deren jeweilige in Bezug auf die in den Anhängen I und II genannten Einrichtungen vorgesehenen Aufgaben mit.

(8) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Einsetzung nationaler CSIRTs ersuchen.

Artikel 10

Anforderungen an die CSIRTs 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. Die CSIRTs 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 müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft gewährleisten können;

e) Die CSIRTs müssen über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die Kontinuität ihrer Dienste zu sicherzustellen;

f) Die CSIRTs müssen die Möglichkeit haben, sich an internationalen Kooperationsnetzen zu beteiligen.

(2) Die CSIRTs haben folgende Aufgaben:

a) Überwachung von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene;

b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie **zuständige Behörden und** andere interessierte Kreise;

c) Reaktion auf Sicherheitsvorfälle;

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

e) [...] Durchführung einer proaktiven Überprüfung der [...] Netz- und Informationssysteme **mit dem Ziel,** Schwachstellen **mit potenziell erheblichen Auswirkungen zu erkennen, unter der Voraussetzung, dass bei fehlender Zustimmung der betreffenden Einrichtung weder in die Netz- und Informationssysteme eingedrungen noch ihre Funktionsweise beeinträchtigt wird**;

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

fa) gegebenenfalls Wahrnehmung der Rolle eines Koordinators für die Zwecke des Verfahrens der koordinierten Offenlegung von Schwachstellen gemäß Artikel 6 Absatz 1; dazu gehört insbesondere die Erleichterung von Interaktionen zwischen den meldenden Einrichtungen, dem für die potenzielle Schwachstelle Verantwortlichen und dem Hersteller oder Anbieter von IKT-Produkten oder -Diensten, wenn dies erforderlich ist, die Ermittlung von und Kontaktaufnahme zu meldenden Einrichtungen, die Aushandlung von Offenlegungsfristen und das Management von Schwachstellen, die mehrere Organisationen betreffen (koordinierte Offenlegung von Schwachstellen, die mehrere Parteien betreffen).

(3) Die CSIRTs bauen Kooperationsbeziehungen mit einschlägigen Akteuren des Privatsektors auf, um die Ziele der Richtlinie besser erreichen zu können.

(3a) Die CSIRTs können Kooperationsbeziehungen zu nationalen CSIRTs von Drittländern aufbauen. Im Rahmen dieser Zusammenarbeit können sie im Einklang mit den Datenschutzvorschriften der Union relevante Informationen, einschließlich personenbezogener Daten, austauschen.

(4) Zur Erleichterung der Zusammenarbeit fördern die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Verfahren für Klassifizierungssysteme und Taxonomien für

a) Verfahren zur Bewältigung von Sicherheitsvorfällen,

b) das Cybersicherheitskrisenmanagement,

c) die koordinierte Offenlegung von Schwachstellen.

Artikel 11

Zusammenarbeit auf nationaler Ebene

(1) Handelt es sich bei den zuständigen Behörden gemäß Artikel 8, der zentralen Anlaufstelle und dem/den CSIRT(s) 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 Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen gemäß dieser Richtlinie entweder ihren zuständigen Behörden oder ihren CSIRTs übermittelt werden. Entscheidet ein Mitgliedstaat, dass diese Meldungen nicht an seine CSIRTs zu richten sind, so wird den CSIRTs in dem zur Wahrnehmung ihrer Aufgaben erforderlichen Umfang Zugang zu den Daten über Sicherheitsvorfälle gewährt, die gemäß Artikel 20 von wesentlichen oder wichtigen Einrichtungen gemeldet werden.

(3) Jeder Mitgliedstaat stellt sicher, dass seine zuständigen Behörden oder CSIRTs seine zentrale Anlaufstelle über gemäß dieser Richtlinie vorgenommene Meldungen von Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen unterrichten.

(4) Soweit dies zur wirksamen Wahrnehmung der in dieser Richtlinie festgelegten Aufgaben und Pflichten erforderlich ist, sorgen die Mitgliedstaaten für eine angemessene Zusammenarbeit zwischen den zuständigen Behörden**, den CSIRTS,** den zentralen Anlaufstellen sowie den Strafverfolgungsbehörden, den Datenschutzbehörden, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] **benannten zuständigen Behörden, den gemäß der Durchführungsverordnung 2019/1583 der Kommission** zuständigen Behörden**, den im Einklang mit der Richtlinie (EU) 2018/1972 benannten Regulierungsbehörden, den gemäß Artikel 17 der Verordnung (EU) Nr. 910/2014 benannten nationalen Behörden,** den gemäß der Verordnung (EU) XXXX/XXXX des Europäischen Parlaments und des Rates [DORA-Verordnung] [...] benannten nationalen Finanzbehörden **sowie den in dem jeweiligen Mitgliedstaat durch andere sektorspezifische Rechtsakte der Union benannten zuständigen Behörden**.

(5) Die Mitgliedstaaten stellen sicher, dass ihre **gemäß dieser Richtlinie** zuständigen Behörden **und** die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden regelmäßig **Informationen** über **die Ermittlung kritischer Einrichtungen,** Cybersicherheitsrisiken, Cyberbedrohungen und Sicherheitsvorfälle **sowie über nicht cyberbezogene Risiken, Bedrohungen und Vorfälle**, die als kritisch **ermittelte wesentliche** Einrichtungen **[**oder kritischen Einrichtungen gleichgestellte Einrichtungen**]** gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] [...] betreffen, sowie über die [...] als Reaktion auf diese Risiken und Sicherheitsvorfälle ergriffenen Maßnahmen **austauschen**. **Darüber hinaus stellen die Mitgliedstaaten sicher, dass die gemäß dieser Richtlinie zuständigen Behörden und die gemäß der Verordnung XXXX/XXXX [DORA-Verordnung], der Richtlinie (EU) 2018/1972 und der Verordnung (EU) Nr. 910/2014 benannten Behörden regelmäßig einschlägige Informationen austauschen.**

In Bezug auf Vertrauensdiensteanbieter und insbesondere in Fällen, in denen diese Aufsichtsfunktion gemäß dieser Richtlinie einer anderen Stelle als den gemäß der Verordnung (EU) Nr. 910/2014 benannten Aufsichtsstellen übertragen wird, arbeiten die nach dieser Richtlinie zuständigen nationalen Behörden zeitnah und eng zusammen, indem sie die einschlägigen Informationen austauschen, um eine wirksame Aufsicht und Einhaltung der Anforderungen dieser Richtlinie und der Verordnung [XXXX/XXXX] durch die Vertrauensdiensteanbieter zu gewährleisten; gegebenenfalls unterrichten die nach dieser Richtlinie zuständigen nationalen Behörden zudem unverzüglich die Aufsichtsstellen gemäß der eIDAS-Verordnung über gemeldete erhebliche Cyberbedrohungen oder Vorfälle mit Auswirkungen auf Vertrauensdienste.

(5a) Um die Meldung von Sicherheitsvorfällen zu vereinfachen, können die Mitgliedstaaten eine zentrale Anlaufstelle für alle Meldungen einrichten, die gemäß dieser Richtlinie sowie gegebenenfalls nach der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG vorgeschrieben sind. Die Mitgliedstaaten können die zentrale Anlaufstelle auch für Meldungen nutzen, die im Rahmen anderer sektorspezifischer Rechtsakte der Union vorgeschrieben sind. Die Anwendung der Bestimmungen der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, insbesondere der Bestimmungen über unabhängige Aufsichtsbehörden, bleiben von diesen zentralen Anlaufstelle unberührt.

KAPITEL III

EU-Zusammenarbeit

Artikel 12

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 6 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 gemäß der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] benannten zuständigen Behörden** können sich gemäß Artikel **42** [...] Absatz **1** [...] der Verordnung (EU) XXXX/XXXX [DORA-Verordnung] an den Tätigkeiten der Kooperationsgruppe beteiligen.

Gegebenenfalls kann die Kooperationsgruppe 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;

aa) Bereitstellung von Orientierungshilfen für die Ausarbeitung und Umsetzung von Maßnahmen zur koordinierten Offenlegung von Schwachstellen gemäß Artikel 5 Absatz 2 Buchstabe c und Artikel 6 Absatz 1;

b) Austausch bewährter Verfahren und Informationsaustausch im Zusammenhang mit der Umsetzung dieser Richtlinie, auch in Bezug auf Cyberbedrohungen, Sicherheitsvorfälle, Schwachstellen, Beinahe-Vorfälle, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau sowie Normen und technische Spezifikationen;

c) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit;

d) beratender Austausch und Zusammenarbeit mit der Kommission bei Entwürfen von Durchführungsrechtsakten [...] der Kommission, die gemäß dieser Richtlinie erlassen werden;

e) Austausch bewährter Verfahren und Informationsaustausch mit den einschlägigen Organen, Einrichtungen, Ämtern und Agenturen der Union;

ea) Meinungsaustausch über die Umsetzung sektorspezifischer Rechtsvorschriften, die Aspekte der Cybersicherheit enthalten;

f) Erörterung von Berichten über das in Artikel 16 Absatz 7 genannte Peer [...] **-Learning**;

g) Erörterung von **Erfahrungen aus** [...] den gemeinsamen Aufsichtstätigkeiten in grenzübergreifenden Fällen gemäß Artikel 34;

h) Bereitstellung strategischer Orientierungshilfen für das CSIRT-Netzwerk **und EU–CyCLONe** zu spezifischen neu auftretenden Fragen;

ha) Meinungsaustausch über politische Folgemaßnahmen zu großen Cybersicherheitsvorfällen auf der Grundlage der im Rahmen des CSIRT-Netzwerks und von EU-CyCLONe gesammelten Erfahrungen;

i) 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 der Mitgliedstaaten beteiligen;

j) Organisation regelmäßiger gemeinsamer Sitzungen mit einschlägigen interessierten Kreisen des Privatsektors aus der gesamten Union, um die Tätigkeiten der Gruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen;

k) Erörterung der Arbeiten im Zusammenhang mit Cybersicherheitsübungen, einschließlich der Arbeit der ENISA**;** [...]

ka) Einrichtung des Peer-Learning-Mechanismus gemäß Artikel 16 dieser Richtlinie.

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

(6) Die Kooperationsgruppe erstellt bis zum … [24 Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre ein Arbeitsprogramm mit den zur Umsetzung ihrer Ziele und Aufgaben zu ergreifenden Maßnahmen. Der Zeitrahmen des ersten gemäß dieser Richtlinie angenommenen Programms wird an den Zeitrahmen des letzten gemäß der Richtlinie (EU) 2016/1148 angenommenen Programms angepasst.

(7) Die Kommission kann Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten erlassen, die für das Funktionieren der Kooperationsgruppe erforderlich sind. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

(8) Die Kooperationsgruppe tagt regelmäßig, mindestens aber einmal jährlich gemeinsam mit der mit der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit **zu fördern** und den Informationsaustausch zu **erleichtern** [...].

Artikel 13

CSIRT-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 der nationalen CSIRTs errichtet.

(2) Das CSIRT-Netzwerk setzt sich aus **gemäß Artikel 9 benannten** Vertretern der CSIRTs der Mitgliedstaaten und **Vertretern** des CERT-EU zusammen. Die Kommission nimmt als Beobachterin am CSIRT-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und unterstützt aktiv die Zusammenarbeit zwischen den CSIRTs.

(3) Das CSIRT-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Kapazitäten der CSIRTs;

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

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

bb) Austausch technischer Lösungen zur Erleichterung der technischen Bewältigung von Sicherheitsvorfällen;

bc) Austausch bewährter Verfahren, Instrumente und Verfahren im Zusammenhang mit den Aufgaben der CSIRTs;

c) auf Antrag eines potenziell von einem Sicherheitsvorfall betroffenen [...] **Mitglieds** des CSIRT-Netzwerkes Austausch und Erörterung von Informationen über diesen Sicherheitsvorfall und die damit verbundenen Cyberbedrohungen, Risiken und Schwachstellen;

d) auf Antrag eines [...] **Mitglieds** des CSIRT-Netzwerkes Erörterung und, sofern möglich, Umsetzung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet seines Mitgliedstaats festgestellt wurde;

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

f) Zusammenarbeit mit, **Austausch bewährter Verfahren mit** und Unterstützung von gemäß Artikel 6 benannten CSIRTs im Hinblick auf das Vorgehen bei einer [...] koordinierten Offenlegung von Schwachstellen, von denen mehrere in verschiedenen Mitgliedstaaten niedergelassene Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen betroffen sind;

g) 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 und -krisen gemäß Artikel 7 Absatz 3;

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

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

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

k) Zusammenarbeit und Informationsaustausch mit regionalen und unionsweiten Sicherheitseinsatzzentren, um die gemeinsame Lageerfassung bei Sicherheitsvorfällen und Bedrohungen in der gesamten Union zu verbessern;

l) Erörterung der in Artikel 16 Absatz 7 genannten Berichte über Peer-**Learning** [...];

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

(4) Für die Zwecke der Überprüfung gemäß Artikel 35 bewertet das CSIRT-Netzwerk bis zum [24 Monate nach Inkrafttreten dieser Richtlinie] und danach alle zwei Jahre die Fortschritte bei der operativen Zusammenarbeit und erstellt einen Bericht. Der Bericht muss insbesondere Schlussfolgerungen zu den Ergebnissen des Peer-**Learning** [...] gemäß Artikel 16 enthalten, die in Bezug auf nationale CSIRTs durchgeführt wurden, einschließlich der Schlussfolgerungen und Empfehlungen gemäß dem genannten Artikel. Dieser Bericht wird auch der Kooperationsgruppe übermittelt.

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

(6) Das CSIRT-Netzwerk arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit EU-CyCLONe zusammen.

Artikel 14

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

(1) Zur Unterstützung des koordinierten Managements massiver Cybersicherheitsvorfälle und -krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Informationsaustauschs zwischen den Mitgliedstaaten und den Organen, Einrichtungen und Agenturen der Union wird hiermit 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 gemäß Artikel 7 benannten für das **Cyberk**risenmanagement zuständigen Behörden der Mitgliedstaaten [...] zusammen. **Die Kommission beteiligt sich als Beobachterin an den Tätigkeiten des Netzwerks.** ENISA führt die Sekretariatsgeschäfte des Netzwerks**,** [...] 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 EU-CyCLONe Vertreter der maßgeblichen Interessenträger einladen, an ihren Arbeiten teilzunehmen.

(3) EU-CyCLONe hat folgende Aufgaben:

a) Verbesserung der Vorsorge im Hinblick auf das Management massiver **Cybers**icherheitsvorfälle und -krisen;

b) Entwicklung einer gemeinsamen Lageerfassung für [...] **massive Cybersicherheitsvorfälle und -krisen;**

ba) Bewertung der Folgen und Auswirkungen relevanter massiver Cybersicherheitsvorfälle und Vorschläge für mögliche Abhilfemaßnahmen;

c) Koordinierung des Managements massiver **Cybers**icherheitsvorfälle und -krisen sowie Unterstützung der Entscheidungsfindung auf politischer Ebene in Bezug auf solche Sicherheitsvorfälle und Krisen;

d) **auf Ersuchen eines Mitgliedstaats** Erörterung **seines** [...] nationalen Plans für die Reaktion auf Cybersicherheitsvorfälle **und -krisen** gemäß Artikel 7 Absatz **3** [...].[...]

(4) EU-CyCLONe gibt sich eine Geschäftsordnung.

(5) EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über **das Management massiver Cybersicherheitsvorfälle und -krisen** [...], wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.

(6) EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten mit dem CSIRT-Netzwerk zusammen.

(7) EU-CyCLONe legt dem Europäischen Parlament und dem Rat bis zum [24 Monate nach Inkrafttreten dieser Richtlinie] einen Bericht vor, in dem seine Arbeit bewertet wird.

Artikel 13a

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 CSIRT-Netzwerk und EU-CyCLONe im Einklang mit dem Datenschutzrecht der Union ermöglicht und geregelt wird.

Artikel 15

Bericht über den Stand der Cybersicherheit in der Union

(1) Die ENISA veröffentlicht in Zusammenarbeit mit der Kommission **und der Kooperationsgruppe** einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union. Dieser Bericht muss insbesondere Folgendes enthalten:

aa) eine Bewertung der Cybersicherheitsrisiken auf Unionsebene unter Berücksichtigung der Bedrohungslage;

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

b) [...]

c) [...] eine **auf quantitativen und qualitativen Indikatoren für die Cybersicherheit beruhende** aggregierte Bewertung**, die einen Überblick über den** Entwicklungsstand der Cybersicherheitskapazitäten**, einschließlich sektorspezifischer Kapazitäten, gibt**.

(2) Der Bericht muss insbesondere politische Empfehlungen zur 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 umfassen.

Artikel 16

Peer-Learning

(1) **Um das gegenseitige Vertrauen zu erhöhen, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die für eine wirksame Umsetzung dieser Richtlinie erforderlichen Kapazitäten und Maßnahmen der Mitgliedstaaten im Bereich der Cybersicherheit zu stärken, legt die Kooperationsgruppe mit Unterstützung der Kommission und nach** [...] Konsultation [...] der ENISA **und gegebenenfalls des CSIRT-Netzwerks** [...] spätestens [...] **24** Monate nach Inkrafttreten dieser Richtlinie die Methode [...] eines **objektiven, nichtdiskriminierenden und fairen** Peer-**Learning**[...]-Systems **für die Umsetzung dieser Richtlinie durch die** [...] Mitgliedstaaten fest. **Die Teilnahme am Peer-Learning ist freiwillig. Das System besteht aus Bewertungsrunden,** die [...] von [...] Sachverständigen für Cybersicherheit aus [...] den [...] Mitgliedstaaten durchgeführt **werden,** und erstreckt sich [...] auf [...] **einen oder mehrere der folgenden Aspekte**:

i) die [...] Umsetzung der Anforderungen an das Cybersicherheitsrisikomanagement und der Meldepflichten gemäß den Artikeln 18 und 20;

ii) [...] **die** Kapazitäten, einschließlich der verfügbaren [...] Ressourcen, und die [...] Durchführung der Aufgaben der **in Artikel 8 genannten** zuständigen nationalen Behörden **und der in Artikel 9 genannten CSIRTs**;

[...]

i**ii** [...]) die [...] **Umsetzung** der Amtshilfe gemäß Artikel 34;

iv) die [...] **Umsetzung** des in Artikel 26 [...] genannten Rahmens für den Informationsaustausch.

(2) **Die** [...] Kriterien [...], anhand deren die Mitgliedstaaten Sachverständige benennen, die für die [...] **Beteiligung an den Peer-Learning-Runden** infrage kommen [...]**, müssen objektiv, nichtdiskriminierend, fair und transparent sein und werden in die in Absatz 1 genannte Methode einbezogen**. Die ENISA und die Kommission **können** Sachverständige benennen, die als Beobachter an den [...] **Peer-Learning-Runden** teilnehmen. [...]

(3) [...] .

(3a) Vor Beginn einer Peer-Learning-Runde können die Mitgliedstaaten eine Eigenbewertung der Aspekte dieser Peer-Learning-Runde durchführen und diese Bewertung den in Absatz 2 genannten benannten Experten zur Verfügung stellen.

(4) [...] **Das** Peer [...] **-Learning kann physische** oder virtuelle Besuche am Standort und Möglichkeiten zum Austausch außerhalb des Standorts umfassen. In Anbetracht des Grundsatzes der guten Zusammenarbeit stellen die **am Peer-Learning beteiligten** [...] Mitgliedstaaten den benannten Sachverständigen die für die Bewertung [...] erforderlichen Informationen zur Verfügung**, vorbehaltlich der Rechtsvorschriften der Mitgliedstaaten oder der Union über den Schutz vertraulicher oder als Verschlusssachen eingestufter Informationen oder der Wahrung grundlegender Funktionen des Staates wie der nationalen Sicherheit**. Sämtliche durch das Peer-**Learning**[...]-Verfahren erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die am Peer-**Learning** [...] beteiligten Sachverständigen geben keine sensiblen oder vertraulichen Informationen, die **in diesem Rahmen** [...] erlangt wurden, an Dritte weiter. **Der am Peer-Learning beteiligten Mitgliedstaat kann Einwände gegen die Benennung bestimmter Sachverständiger erheben, wenn dies hinreichend begründet ist und der Kooperationsgruppe mitgeteilt wird.**

(5) Nach Abschluss einer Peer-**Learning-Runde** [...] dürfen in den **vier** [...] Jahren danach **für den beteiligten** [...] Mitgliedstaat keine weiteren **Peer-Learning-Runden** zu denselben Aspekten durchgeführt werden, es sei denn, [...] **der betreffende Mitgliedstaat ersucht darum oder stimmt einem entsprechenden Vorschlag der Kooperationsgruppe zu**.

(6) [...]

(7) Die an Peer-**Learning-Runden** beteiligten Sachverständigen erstellen Berichte über die Ergebnisse und Schlussfolgerungen der **Bewertungen** [...]. **Die Mitgliedstaaten können Bemerkungen zu dem sie jeweils betreffenden Berichtsentwurf übermitteln, die dem Bericht beigefügt werden.** Die **endgültigen** Berichte werden [...] der Kooperationsgruppe [...] vorgelegt**; die Mitgliedstaaten können beschließen, dass der sie jeweils betreffende Bericht veröffentlicht wird**.

KAPITEL IV

Risikomanagement und Meldepflichten im Bereich Cybersicherheit

ABSCHNITT I

Risikomanagement und Meldungen im Bereich Cybersicherheit

Artikel 17

Governance

(1) Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 18 ergriffenen Maßnahmen zum Cybersicherheitsrisikomanagement billigen, **dessen** Umsetzung **überwachen** [...] und für die Nichteinhaltung der Verpflichtungen nach diesem Artikel durch die betreffenden Einrichtungen [...] **zur Rechenschaft gezogen werden können**.

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

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane regelmäßig an [...] Schulungen teilnehmen **müssen**, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf den Betrieb der Einrichtung zu erwerben.

Artikel 18

Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1a) **In Rahmen dieser Richtlinie wird ein „gefahrenübergreifender“ Ansatz verfolgt, der den Schutz von Netz- und Informationssystemen und ihres physischen Umfelds vor allen Ereignissen umfasst, 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.**

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen bei der Erbringung ihrer Dienste nutzen, zu beherrschen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik **und der Durchführungskosten** 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, ihre Größe, die Wahrscheinlichkeit des Auftretens von Vorfällen und deren Schweregrad besonders zu berücksichtigen. Unter Berücksichtigung der Höhe und der Art des Risikos für die Gesellschaft im Falle von Sicherheitsvorfällen, die wesentliche oder wichtige Einrichtungen betreffen, können die Maßnahmen zum Cybersicherheitsrisikomanagement, die wichtigen Einrichtungen auferlegt werden, weniger streng sein als die Maßnahmen, die wesentlichen Einrichtungen auferlegt werden.**

(2) Die in Absatz 1 genannten Maßnahmen müssen zumindest Folgendes umfassen:

a) Risikoanalyse- und Sicherheitskonzepte für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen (Prävention, Erkennung**,** [...] Reaktion [...] **und Wiederherstellung bei** Sicherheitsvorfällen);

c) Aufrechterhaltung des Betriebs und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren **Direkta**nbietern oder Diensteanbietern beispielsweise Anbietern von Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS);

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) **Konzept für den** Einsatz von Kryptografie und Verschlüsselung.

ga) Gewährleistung der Sicherheits des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen.

(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die spezifischen Schwachstellen der einzelnen **Direkta**nbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen **müssen**. **Die Mitgliedstaaten stellen ferner sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d die Ergebnisse der gemäß Artikel 19 Absatz 1 durchgeführten koordinierten Risikobewertungen berücksichtigen müssen.**

(4) Die Mitgliedstaaten stellen sicher, dass Einrichtungen, die feststellen, dass ihre Dienste oder Aufgaben die Anforderungen nach Absatz 2 nicht erfüllen, unverzüglich alle erforderlichen Korrekturmaßnahmen ergreifen, um den betreffenden Dienst mit den Anforderungen in Einklang zu bringen.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, um die technischen und methodischen Spezifikationen **sowie erforderlichenfalls sektorenspezifische Besonderheiten** für die in Absatz 2 genannten Elemente festzulegen. **Die Kommission erlässt bis zum [18 Monate nach Inkrafttreten dieser Richtlinie] Durchführungsrechtsakte, um die technischen und methodischen Spezifikationen für die Einrichtungen nach Artikel 24 Absatz 1 und die Vertrauensdiensteanbieter nach Anhang I Nummer 8 festzulegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.** Bei der Ausarbeitung dieser **Durchführungsr**echtsakte **beachtet** die Kommission [...] so weit wie möglich internationale und europäische Normen sowie die einschlägigen technischen Spezifikationen **und steht gemäß Artikel 12 Absatz 4 Buchstabe d in einem beratenden Austausch mit der Kooperationsgruppe und der ENISA über die Entwürfe von Durchführungsrechtsakten**.

(6) [...]

Artikel 19

EU-weit koordinierte Risikobewertungen kritischer Lieferketten

(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 fest, welche spezifischen kritischen IKT-Dienste, -Systeme oder -Produkte der koordinierten Risikobewertung nach Absatz 1 unterzogen werden können.

Artikel 20

Meldepflichten

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder dem CSIRT gemäß den Absätzen 3 und 4 unverzüglich jeden Sicherheitsvorfall melden, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste hat. Gegebenenfalls unterrichten diese Einrichtungen die Empfänger ihrer Dienste unverzüglich über **diese** Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Mitgliedstaaten stellen sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es den zuständigen Behörden oder dem CSIRT ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat. **Mit der Meldungshandlung an sich wird keine höhere Haftung der meldenden Einrichtung begründet.**

(2) [...]

Gegebenenfalls unterrichten [...] **die wesentlichen und wichtigen** Einrichtungen die potenziell von einer erheblichen Cyberbedrohung betroffenen Empfänger ihrer Dienste unverzüglich über alle Maßnahmen oder Abhilfemaßnahmen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die Bedrohung selbst. Mit der Meldung**shandlung an sich** wird keine höhere Haftung der meldenden Einrichtung begründet.

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

a) der Sicherheitsvorfall [...] **schwerwiegende Störungen des Betriebs des Dienstes** oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder potenziell verursachen könnte;

b) der Sicherheitsvorfall andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Verluste geschädigt hat oder potenziell schädigen könnte.

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

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des Sicherheitsvorfalls, eine erste Meldung **als Frühwarnung**, in der gegebenenfalls angegeben wird, ob der Sicherheitsvorfall vermutlich auf rechtswidrige oder böswillige Handlungen zurückzuführen ist;

b) auf Ersuchen einer zuständigen Behörde oder eines CSIRT einen Zwischenbericht über relevante Statusaktualisierungen;

c) spätestens einen Monat nach **Übermittlung der ersten Meldung** [...] gemäß Buchstabe a einen Abschlussbericht, der mindestens Folgendes enthält:

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

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

iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen.

Die Mitgliedstaaten sehen vor, dass die betreffende Einrichtung in hinreichend begründeten Fällen und im Einvernehmen mit den zuständigen Behörden oder dem CSIRT von den unter den Buchstaben a und c festgelegten Fristen abweichen kann. **Insbesondere kann eine Abweichung von der in Buchstabe c genannten Frist gerechtfertigt sein, wenn der Vorfall noch andauert.**

(5) Die zuständigen nationalen Behörden oder das CSIRT übermitteln der meldenden Einrichtung [...] nach Eingang der ersten Meldung gemäß Absatz 4 Buchstabe a **unverzüglich** eine Antwort, einschließlich einer ersten Rückmeldung zu dem Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen für die Durchführung möglicher Abhilfemaßnahmen. Wurde die in Absatz 1 genannte Meldung nicht dem CSIRT übermittelt, 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 Sicherheitsvorfall ein krimineller Hintergrund vermutet, geben die zuständigen nationalen Behörden oder das CSIRT ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

(6) Gegebenenfalls und insbesondere, wenn der in Absatz 1 genannte Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet die zuständige Behörde**,** [...] das CSIRT **oder die zentrale Anlaufstelle** die anderen betroffenen Mitgliedstaaten und die ENISA über den Sicherheitsvorfall. **Diese Informationen müssen mindestens die in Absatz 4 aufgeführten Elemente enthalten.** Dabei wahren die zuständigen Behörden, die CSIRTs und die zentralen Anlaufstellen im Einklang mit dem Unionsrecht oder mit den dem Unionsrecht entsprechenden nationalen Rechtsvorschriften die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

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

(8) Auf Ersuchen der zuständigen Behörde oder des CSIRT 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 sechs Monate** einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß [...] **Absatz** 1 [...] und gemäß Artikel 27 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben herausgeben. **Die ENISA unterrichtet die Kooperationsgruppe und das CSIRT-Netzwerk alle sechs Monate über ihre Erkenntnisse zu den eingegangenen Meldungen.**

(10) Die zuständigen Behörden stellen den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden Informationen über Sicherheitsvorfälle und Cyberbedrohungen zur Verfügung, die nach den Absätzen 1 und 2 von wesentlichen Einrichtungen, die im Sinne der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen **[**oder als kritischen Einrichtungen gleichwertige Einrichtungen**]** gelten, gemeldet wurden.

(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß den Absätzen 1 und 2 näher bestimmt werden. Die Kommission kann ferner Durchführungsrechtsakte erlassen, um genauer zu bestimmen, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne des Absatzes 3 anzusehen ist. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 21

Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung

(1) Die Mitgliedstaaten können [...] Einrichtungen dazu verpflichten, bestimmte IKT-Produkte, -Dienste und -Prozesse**, die** im Rahmen spezifischer **gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommener** europäischer Systeme für die Cybersicherheitszertifizierung [...] **zertifiziert wurden, zu nutzen**, um die Erfüllung bestimmter in Artikel 18 genannter Anforderungen nachzuweisen. Die [...] **zertifizierten IKT-**Produkte, **-Dienste** [...] und **-**Prozesse können von einer wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft worden sein.

(2) Der Kommission **kann** [...] delegierte Rechtsakte [...] erlassen, in denen ausgeführt wird, welche Kategorien wesentlicher **oder wichtiger** Einrichtungen **bestimmte IKT-Produkte, -Dienste und -Prozesse nutzen** oder ein Zertifikat erlangen müssen und welche [...] **gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommenen** europäischen Systeme für die Cybersicherheitszertifizierung dabei anzuwenden sind. **Diese Durchführungsrechtsakte werden gemäß dem in Artikel 37 Absatz 2 genannten Prüfverfahren erlassen. Bei Ausarbeitung dieser Durchführungsrechtsakte verfährt die Kommission gemäß Artikel 56 der Verordnung (EU) 2019/881wie folgt:**

i) 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 und der Verfügbarkeit von Alternativen auf dem Markt ergibt;

ii) sie führt eine offene, transparente und inklusive Konsultation mit allen relevanten Interessenträgern und mit den Mitgliedstaaten durch;

(iii) sie berücksichtigt die Umsetzungsfristen sowie die Übergangsmaßnahmen oder -zeiträume und insbesondere in Hinblick auf die möglichen Auswirkungen der Maßnahmen auf die Anbieter oder Hersteller von IKT-Produkten, -Diensten und -Prozessen, insbesondere KMU;

(iv) sie berücksichtigt das Bestehen und die Umsetzung einschlägiger Rechtsvorschriften der Mitgliedstaaten.

(3) Ist kein geeignetes europäisches System für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 **des vorliegenden Artikels** vorhanden, kann die Kommission die ENISA auffordern, gemäß Artikel 48 Absatz 2 der Verordnung (EU) 2019/881 ein vorläufiges System auszuarbeiten **oder ein bestehendes europäisches System für die Cybersicherheitszertifizierung zu überarbeiten**.

Artikel 22

Normung

(1) Um die einheitliche Anwendung des Artikels 18 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

(2) In Zusammenarbeit mit den Mitgliedstaaten 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 der Mitgliedstaaten —, mit denen diese Bereiche abgedeckt werden könnten.

Artikel 23

Datenbanken der Domänennamen und Registrierungsdaten

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, stellen die Mitgliedstaaten sicher, dass die TLD-**Namenr**egister und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank sammeln und pflegen, wobei [...] **sie ihren Sorgfaltspflichten gemäß den** Datenschutzvorschriften der Union in Bezug auf personenbezogene Daten [...] **nachkommen**.

(2) Die Mitgliedstaaten stellen sicher, dass die Datenbanken zu den in Absatz 1 genannten Domänennamen-Registrierungsdaten einschlägige Informationen enthalten, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können [...] **und die mindestens Folgende Angaben umfassen:**

a) Domänenname;

b) Datum der Registrierung;

c) Registrierungsdaten, darunter

i) für Einzelpersonen – Name, Vorname und E-Mail-Adresse,

ii) für juristische Personen – Name und E-Mail-Adresse.

(3) Die Mitgliedstaaten stellen sicher, dass die TLD-**Namenr**egister und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, über Vorgaben und Verfahren verfügen, mit denen sichergestellt wird, dass die Datenbanken genaue und vollständige Angaben enthalten. Die Mitgliedstaaten stellen sicher, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.

(4) Die Mitgliedstaaten stellen sicher, dass die TLD-**Namenr**egister und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänenregistrierungsdaten veröffentlichen.

(5) Die Mitgliedstaaten stellen sicher, dass die TLD-**Namenr**egister und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten stellen sicher, dass die TLD-**Namen**register und die Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen, alle Anträge auf Zugang unverzüglich**, in jedem Fall aber innerhalb von 72 Stunden** beantworten. Die Mitgliedstaaten stellen sicher, dass die Vorgaben und Verfahren für die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

Abschnitt II

Gerichtliche Zuständigkeit und Registrierung

Artikel 24

Gerichtliche Zuständigkeit und Territorialität

(1a) Es gilt, dass wesentliche und wichtige Einrichtungen, die unter diese Richtlinie fallen, der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Dienste erbringen. Es gilt, dass Einrichtungen gemäß Anhang I Nummern 1 bis 7 und 10, Vertrauensdiensteanbieter und Betreiber von Internet-Knoten gemäß Anhang I Nummer 8 und Einrichtungen gemäß Anhang II Nummern 1 bis 5 der gerichtlichen Zuständigkeit des Mitgliedstaats im Hoheitsgebiet unterliegen, in dem sie niedergelassen sind.

(1) Es gilt, dass DNS-Diensteanbieter, TLD-Namenregister, **Einrichtungen, die Domänennamen-Registrierungsdienste für die TLD erbringen,** Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten**,** [...] Betreiber von Inhaltszustellnetzen**, Anbieter verwalteter Dienste und Anbieter verwalteter Sicherheitsdienste** gemäß Anhang I Nummer 8 **und Nummer 8a** sowie Anbieter digitaler Dienste gemäß Anhang II Nummer 6 der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem sie ihre Hauptniederlassung in der Union haben.

(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union der in Absatz 1 genannten Einrichtungen jeweils die Niederlassung in demjenigen Mitgliedstaat gilt, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement **vorwiegend** getroffen werden. **Kann der Ort, an dem solche Entscheidungen vorwiegend getroffen werden, nicht bestimmt werden oder w**erden solche Entscheidungen in keiner Niederlassung in der Union getroffen, wird davon ausgegangen, dass sich die Hauptniederlassung der Einrichtung in dem Mitgliedstaat befindet, in dem die Niederlassung mit der höchsten Beschäftigtenzahl in der Union angesiedelt ist. **Werden die Dienste von einer Unternehmensgruppe angeboten, so gilt die Hauptniederlassung als Hauptniederlassung der Unternehmensgruppe.**

(3) Hat eine in Absatz 1 genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienstleistungen 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 gilt, dass solche Einrichtungen der gerichtlichen Zuständigkeit des Mitgliedstaats unterliegen, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Artikels benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen Nichteinhaltung der Verpflichtungen nach dieser Richtlinie einleiten.

(4) Die Benennung eines Vertreters durch eine in Absatz 1 genannte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

(4a) Mitgliedstaaten, die ein Amtshilfeersuchen zu in Absatz 1 genannten Einrichtungen erhalten haben, können innerhalb der Grenzen des 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 25

Register für bestimmte Einrichtungen für digitale Infrastruktur und Anbieter digitaler Dienste

(1) [...] **Die Mitgliedstaaten stellen sicher, dass die in Artikel 24 Absatz 1 genannten** Einrichtungen**, deren Hauptniederlassung sich in ihrem Hoheitsgebiet befindet oder, falls sie nicht in der Union niedergelassen sind, deren benannter Vertreter in der Union in ihrem Hoheitsgebiet niedergelassen ist, der zuständigen Behörde** [...] spätestens bis zum … [12 Monate nach Inkrafttreten der Richtlinie] folgende Angaben übermitteln:

a) Name der Einrichtung;

aa) die Art der Einrichtung gemäß den Anhängen I und II dieser Richtlinie;

b) 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 24 Absatz 3 benannten Vertreters;

c) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtungen **und ihrer Vertreter;**

d) Mitgliedstaaten, in denen die Einrichtung den Dienst anbietet.

Diese Informationen werden gegebenenfalls im Rahmen des nationalen Eigenmeldungsverfahren gemäß Artikel 2a übermittelt.

(2) **Die Mitgliedstaaten stellen sicher, dass i**m Falle einer Änderung der gemäß Absatz 1 übermittelten Angaben die in Absatz 1 genannten Einrichtungen **zudem** [...] diese Änderung **unverzüglich**, in jedem Fall aber innerhalb von drei Monaten nach Wirksamwerden der Änderung **melden**.

(3) [...] **Die** zentralen Anlaufstellen [...] **der Mitgliedstaaten leiten die in den Absätzen 1 und 2 genannten Informationen an die ENISA** weiter. [...]

(3a) Auf der Grundlage der gemäß Absatz 3 erhaltenen Informationen erstellt und führt die ENISA ein Register für die in Absatz 1 genannten Einrichtungen. Auf Ersuchen der Mitgliedstaaten ermöglicht die ENISA den jeweils zuständigen Behörden den Zugang zum Register, wobei sie gegebenenfalls für die erforderlichen Garantien zum Schutz der Vertraulichkeit der Informationen sorgt.

(4) [...]

KAPITEL V

Informationsaustausch

Artikel 26

Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

(1) [...] **D**ie Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen **freiwillig** relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, **Beinahe-Vorfälle,** Schwachstellen, Gefährdungsindikatoren (indicators of compromise – IoC), Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, sofern

a) dieser Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, aufzudecken, zu bewältigen 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 von Bedrohungen, Eindämmungsstrategien oder Reaktions- und Wiederherstellungsphasen unterstützt werden.

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

(3) Die Mitgliedstaaten [...] **können** Vorschriften festlegen, in denen das Verfahren, die operativen Elemente (einschließlich der Nutzung spezieller IKT-Plattformen), der Inhalt und die Bedingungen der in Absatz 2 genannten Vereinbarungen über den Informationsaustausch bestimmt werden. In diesen Vorschriften [...] **können** auch die Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen sowie operative Elemente, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt werden. Die Mitgliedstaaten unterstützen die Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 5 Absatz 2 Buchstabe g genannten Konzepten.

(4) Wesentliche und wichtige Einrichtungen unterrichten die zuständigen Behörden beim Abschluss von in Absatz 2 genannten Vereinbarungen über den Informationsaustausch oder gegebenenfalls über ihren Rücktritt von solchen Vereinbarungen, sobald dieser wirksam wird.

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

Artikel 27

Freiwillige Meldung relevanter Informationen

(1) Unbeschadet des Artikels 20 stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen den zuständigen Behörden oder den CSIRTs auf freiwilliger Basis alle relevanten Vorfälle, Cyberbedrohungen oder Beinahe-Vorfälle melden können.

(2) Die Mitgliedstaaten stellen sicher, dass unbeschadet des Artikels 3 Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, auf freiwilliger Basis erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle melden können. Bei der Bearbeitung dieser Meldungen werden die Mitgliedstaaten gemäß dem in Artikel 20 vorgesehenen Verfahren tätig. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten. **Vorbehaltlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten** dürfen **f**reiwillige 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.

(3) Freiwillige Meldungen werden nur bearbeitet, wenn diese Bearbeitung keinen unverhältnismäßigen oder unzumutbaren Aufwand für den betreffenden Mitgliedstaat darstellt.

KAPITEL VI

Aufsicht und Durchsetzung

Artikel 28

Allgemeine Aspekte der Aufsicht und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung dieser Richtlinie, insbesondere der Verpflichtungen nach den Artikeln 18**, 20** und 23, wirksam überwachen und die erforderlichen Maßnahmen treffen. **Die Mitgliedstaaten können den zuständigen Behörden gestatten, der Aufsicht Vorrang einzuräumen, wobei diese auf einem risikobasierten Ansatz beruhen muss.**

(2) Bei der Bearbeitung von Sicherheitsvorfällen [...] arbeiten die zuständigen Behörden eng mit den Datenschutzbehörden**, den gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannten zuständigen Behörden, den gemäß der Verordnung (EU) Nr. 910/2014 benannten Aufsichtsstellen und anderen gemäß sektorspezifischen Rechtsakten der Union benannten zuständigen Behörden** zusammen. [...]

(3) 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 öffentliche Verwaltung und bei der Durchsetzung möglicher Sanktionen bei Nichteinhaltung über die geeigneten Befugnisse verfügen, um diese Aufgaben in operativer Unabhängigkeit von den beaufsichtigten Einrichtungen wahrnehmen zu können. Die Mitgliedstaaten können entscheiden, ob diesen Einrichtungen im Einklang mit den nationalen Rahmenbedingungen und der nationalen Rechtsordnung geeignete, verhältnismäßige und wirksame Aufsichts- und Durchsetzungsmaßnahmen auferlegt werden.

Artikel 29

Aufsicht und Durchsetzung 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 **einen risikobasierten Ansatz verfolgen und** befugt sind, in Bezug auf diese Einrichtungen **mindestens** folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich Stichprobenkontrollen;

b) regelmäßige **Sicherheitsp**rüfungen;

c) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;

d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien**, auch in Zusammenarbeit mit der betreffenden Einrichtung, wenn dies aus technischen Gründen erforderlich ist**;

e) Anforderung von Informationen, die für die Bewertung der von der Einrichtung ergriffenen Cybersicherheitsmaßnahmen erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte [...];

f) Anforderung des Zugangs zu Daten, Dokumenten oder sonstigen Informationen, die zur Erfüllung ihrer 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.

(2a) Bei der Wahrnehmung ihrer in Absatz 2 aufgeführten Aufsichtsaufgaben können die zuständigen Behörden Aufsichtsmethoden festlegen, die eine Priorisierung dieser Aufgaben auf der Grundlage eines risikobasierten Ansatzes ermöglichen.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstaben e bis g 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** befugt sind,

a) die Einrichtungen bei Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen zu verwarnen;

b) verbindliche Anweisungen oder Anordnungen zu erteilen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen die in dieser Richtlinie festgelegten Verpflichtungen zu beheben;

c) diese Einrichtungen anzuweisen, das nicht mit den in dieser Richtlinie festgelegten Verpflichtungen zu vereinbarende Verhalten einzustellen und von Wiederholungen abzusehen;

d) diese Einrichtungen anzuweisen, ihre Risikomanagementmaßnahmen und/oder die Erfüllung ihrer Meldepflichten entsprechend bestimmter Vorgaben und innerhalb einer bestimmten Frist mit den in den Artikeln 18 und 20 festgelegten Verpflichtungen in Einklang zu bringen;

e) diese Einrichtungen anzuweisen, die natürliche(n) oder juristische(n) Person(en), für die sie Dienste oder Tätigkeiten erbringen 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) diese Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) [...]

h) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen**, sofern eine solche Bekanntgabe nicht eine dem betreffenden Unternehmen schadende Exposition bewirkt**;

i) [...]

j) je nach den einzelstaatlichen Rechtsvorschriften und den Umständen des Einzelfalls zusätzlich zu den oder anstelle der unter den Buchstaben a bis i dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 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 die 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 die zuständigen Behörden befugt sind,

a) die Zertifizierung oder Genehmigung für einen Teil oder alle von einer wesentlichen Einrichtung erbrachten Dienste oder Tätigkeiten auszusetzen oder **je nach den einzelstaatlichen Rechtsvorschriften** eine Zertifizierungs- oder Genehmigungsstelle **oder ein Gericht** aufzufordern, die Zertifizierung oder Genehmigung auszusetzen;

b) gegen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters Leitungsaufgaben in dieser wesentlichen Einrichtung wahrnehmen, und gegen jede andere natürliche Person, die für den Verstoß Verantwortung trägt, ein vorübergehendes Verbot zur Wahrnehmung von Leitungsaufgaben in dieser Einrichtung zu verhängen oder von den zuständigen Stellen oder Gerichten die Verhängung eines solchen Verbots zu verlangen.

Diese Sanktionen werden nur so lange angewandt, bis die Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Sanktionen verhängt wurden, zu erfüllen.

Die in diesem Absatz vorgesehenen Sanktionen gelten nicht für 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 die in dieser Richtlinie festgelegten Verpflichtungen erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung der in dieser Richtlinie festgelegten Verpflichtungen haftbar gemacht werden können. **Für Einrichtungen der öffentlichen Verwaltung gilt diese Bestimmung unbeschadet der Rechtsvorschriften der Mitgliedstaaten über die Haftung von öffentlichen Bediensteten und von gewählten oder ernannten Amtsträgern**.

(7) Bei der Ergreifung von Durchsetzungsmaßnahmen oder der Verhängung von Sanktionen gemäß den Absätzen 4 und 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. Insbesondere sollten folgende Verstöße als schwerwiegend betrachtet werden: wiederholte Verstöße, unterlassene Meldung oder Behebung von Sicherheitsvorfällen, die eine erhebliche Störung bewirken, Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden, Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes von der zuständigen Behörde angeordnet wurden, sowie Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementanforderungen oder Meldepflichten gemäß den Artikeln 18 und 20.

b) die Dauer des Verstoßes, einschließlich des Wiederholungsaspekts;

c) die Höhe des tatsächlich entstandenen Schadens bzw. entstandener Verluste oder potenzieller Schäden oder Verluste, die hätten verursacht werden können, sofern sich diese feststellen lassen. Bei der Bewertung dieses Aspekts sind unter anderem tatsächliche oder potenzielle finanzielle oder wirtschaftliche Verluste, Auswirkungen auf andere Dienste sowie die Zahl der betroffenen oder potenziell betroffenen Nutzer zu berücksichtigen;

d) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

e) von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des Schadens und/oder der Verluste;

f) Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;

g) Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Person(en) mit den zuständigen Behörden.

(8) Die zuständigen Behörden müssen ihre Durchsetzungsentscheidungen ausführlich begründen. Bevor sie solche Entscheidungen treffen, teilen die zuständigen Behörden den betroffenen Einrichtungen ihre vorläufigen Erkenntnisse mit und räumen ihnen eine angemessene Frist zur Stellungnahme ein**, außer im Fall einer unmittelbaren Gefahr**.

(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 wesentliche Einrichtungen, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] als kritische Einrichtungen **[**oder als einer kritischen Einrichtung gleichgestellte Einrichtungen**]** eingestuft wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden [...] **innerhalb desselben** Mitgliedstaats, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] benannt wurden, unterrichten. [...] **Die** gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] zuständigen Behörden [...] **können gegebenenfalls** die **gemäß der vorliegenden Richtlinie** zuständigen Behörden **ersuchen**, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine **in den Anwendungsbereich der vorliegenden Richtlinie fallende wesentliche Einrichtung ausüben, die gemäß der Richtlinie (EU) XXXX/XXXX [Richtlinie über die Resilienz kritischer Einrichtungen] ebenfalls** als kritische **Einrichtung [**oder als einer kritischen Einrichtung gleichgestellte [...] Einrichtung [...]**] eingestuft wurde**.

(10) Die Mitgliedstaaten stellen sicher, dass ihre gemäß dieser Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die gemäß Artikel 28 der Verordnung (EU) XXXX/XXXX [DORA] als kritischer IKT-Drittanbieter benannt wurden, die Verpflichtungen aus dieser Richtlinie erfüllen, das Aufsichtsforum gemäß Artikel 29 Absatz 1 der Verordnung (EU) XXXX/XXXX [DORA] unterrichten.

(10a) Die Mitgliedstaaten stellen sicher, dass ihre gemäß dieser Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse, mit denen sichergestellt werden soll, dass die gemäß der Verordnung (EU) Nr. 910/2014 als Vertrauensdiensteanbieter benannten Einrichtungen die Verpflichtungen aus dieser Richtlinie erfüllen, die jeweils zuständigen Behörden, die gemäß der Verordnung (EU) Nr. 910/2014 benannt wurden, unterrichten.

Artikel 30

Aufsicht und Durchsetzung in Bezug auf wichtige Einrichtungen

(1) Werden Nachweise oder Hinweise **oder Informationen** dafür vorgelegt, dass eine wichtige Einrichtung **mutmaßlich** ihren Verpflichtungen nach dieser Richtlinie, insbesondere den Artikeln 18 und 20, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden.

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

a) Vor-Ort-Kontrollen und nachträgliche externe Aufsichtsmaßnahmen;

b) gezielte Sicherheitsprüfungen auf der Grundlage von Risikobewertungen oder verfügbaren risikobezogenen Informationen;

c) Sicherheitsscans auf der Grundlage objektiver, **nichtdiskriminierender,** fairer und transparenter Risikobewertungskriterien**, auch in Zusammenarbeit mit der betreffenden Einrichtung, wenn dies aus technischen Gründen erforderlich ist**;

d) Anforderung von Informationen, die für die nachträgliche Bewertung der ergriffenen Cybersicherheitsmaßnahmen erforderlich sind [...];

e) Anforderung auf Zugang zu Daten, Dokumenten und/oder sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind**;** [...]

ea) 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.

(2a) Bei der Wahrnehmung ihrer in Absatz 2 aufgeführten Aufsichtsaufgaben können die zuständigen Behörden Aufsichtsmethoden festlegen, die eine Priorisierung dieser Aufgaben auf der Grundlage eines risikobasierten Ansatzes ermöglichen.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstabe d **bis ea** [...] 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** befugt sind,

a) die Einrichtungen bei Nichteinhaltung der in dieser Richtlinie festgelegten Verpflichtungen zu verwarnen;

b) verbindliche Anweisungen oder Anordnungen zu erteilen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder den Verstoß gegen die in dieser Richtlinie festgelegten Verpflichtungen zu beheben;

c) diese Einrichtungen anzuweisen, das nicht mit den in dieser Richtlinie festgelegten Verpflichtungen zu vereinbarende Verhalten einzustellen, und von Wiederholungen abzusehen;

d) diese Einrichtungen anzuweisen, ihre Risikomanagementmaßnahmen oder die Erfüllung ihrer Meldepflichten entsprechend bestimmter Vorgaben und innerhalb einer bestimmten Frist mit den in den Artikeln 18 und 20 festgelegten Verpflichtungen in Einklang zu bringen;

e) diese Einrichtungen anzuweisen, die natürliche(n) oder juristische(n) Person(en), für die sie Dienste oder Tätigkeiten erbringen 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) diese Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) diese Einrichtungen anzuweisen, Aspekte der Nichteinhaltung ihrer in dieser Richtlinie festgelegten Verpflichtungen entsprechend bestimmter Vorgaben öffentlich bekannt zu machen**, sofern eine solche Bekanntgabe nicht eine dem betreffenden Unternehmen schadenden Exposition bewirkt**;

h) [...]

i) je nach den einzelstaatlichen Rechtsvorschriften und den Umständen des Einzelfalls zusätzlich zu den oder anstelle der unter den Buchstaben a bis i dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 31 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Artikel 29 Absätze 6 bis 8 gelten auch für die Aufsichts- und Durchsetzungsmaßnahmen, die in diesem Artikel für die [...] wichtigen Einrichtungen vorgesehen sind.

Artikel 31

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

(1) Die Mitgliedstaaten stellen sicher, dass die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen gemäß diesem Artikel bei Verstößen gegen die in dieser Richtlinie festgelegten Verpflichtungen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h verhängt.

(3) Bei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 29 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

(4) Die Mitgliedstaaten stellen sicher, dass für Verstöße **einer wesentlichen Einrichtung** gegen die Verpflichtungen nach Artikel 18 oder Artikel 20 im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens [...] **4** 000 000 EUR oder **im Falle einer juristischen Person** von [...] 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche [...] Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(4a) Die Mitgliedstaaten stellen sicher, dass für Verstöße einer wichtigen Einrichtung gegen die Verpflichtungen nach Artikel 18 oder Artikel 20 im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 2 000 000 EUR oder im Falle einer juristischen Person von 1 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

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

(6) Unbeschadet der Befugnisse der zuständigen Behörden gemäß den Artikeln 29 und 30 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung im Sinne von Artikel 4 Absatz 23, die den in dieser Richtlinie festgelegten Verpflichtungen unterliegen, Geldbußen verhängt werden können.

(6a) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, stellt dieser Mitgliedstaat sicher, dass dieser Artikel so angewandt werden kann, 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 jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Artikel 32

Verstöße mit Verletzungen des Schutzes personenbezogener Daten

(1) Haben die zuständigen Behörden **im Zuge der Beaufsichtigung oder Durchsetzung erkannt**, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 18 und 20 **dieser Richtlinie** festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Absatz 12 der Verordnung (EU) 2016/679 zur Folge [...] **haben könnte**, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie **unverzüglich** die gemäß den Artikeln 55 und 56 jener Verordnung zuständigen Aufsichtsbehörden [...].

(2) Beschließen die gemäß den Artikeln 55 und 56 der Verordnung (EU) 2016/679 zuständigen Aufsichtsbehörden, ihre Befugnisse gemäß Artikel 58 **Absatz 2** Buchstabe i der genannten Verordnung auszuüben und eine Geldbuße zu verhängen, so dürfen die **in Artikel 8 der vorliegenden Richtlinie genannten** zuständigen Behörden für [...] **einen durch dieselbe Handlung begangenen** Verstoß **gegen** [...] Artikel 31 der vorliegenden Richtlinie keine Geldbuße verhängen. Die zuständigen Behörden können jedoch die Durchsetzungsmaßnahmen oder die Sanktionsbefugnisse gemäß Artikel 29 Absatz 4 Buchstaben a bis i, Artikel 29 Absatz 5 und Artikel 30 Absatz 4 Buchstaben a bis h dieser Richtlinie anwenden bzw. ausüben.

(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so kann die zuständige Behörde die im selben Mitgliedstaat angesiedelte Aufsichtsbehörde davon in Kenntnis setzen.

Artikel 33

Sanktionen

(1) Die Mitgliedstaaten erlassen Vorschriften über Sanktionen für Verstöße gegen die nach dieser Richtlinie erlassenen nationalen Bestimmungen und treffen alle erforderlichen Maßnahmen, um deren Anwendung sicherzustellen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum ... [zwei Jahre nach dem Inkrafttreten dieser Richtlinie] mit und melden ihr unverzüglich etwaige spätere Änderungen daran.

Artikel 34

Amtshilfe

(1) Wenn eine wesentliche oder wichtige Einrichtung ihre Dienste in mehr als einem Mitgliedstaat oder **in einem oder mehreren Mitgliedstaaten** erbringt [...], während 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 betroffenen Mitgliedstaaten über die [...] Aufsichts- und Durchsetzungsmaßnahmen [...] und konsultieren sie zu diesen;

b) eine zuständige Behörde kann eine andere zuständige Behörde ersuchen, die [...] 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** Unterstützung, damit die [...] Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können. Diese 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 nach einem Austausch mit den anderen betroffenen Behörden[...] festgestellt wird, dass die Behörde für die erbetene Amtshilfe nicht zuständig ist **oder nicht über die erforderlichen Ressourcen verfügt** oder dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde [...] steht **oder dass das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, die der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung des betreffenden Mitgliedstaats zuwiderlaufen**.

(2) Die zuständigen Behörden verschiedener Mitgliedstaaten können, wenn angezeigt und im gegenseitigen Einvernehmen die [...] gemeinsamen Aufsichtsmaßnahmen durchführen.

KAPITEL VII

Übergangs- und Schlussbestimmungen

Artikel 35

Überprüfung

Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der in den Anhängen I und II genannten Sektoren, Teilsektoren und Einrichtungen unterschiedlicher Größe und Art für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewertet. [...] **Für die Zwecke der Überprüfung** berücksichtigt die Kommission [...] die Berichte [...] des CSIRT-Netzwerks über die auf [...] operativer Ebene gemachten Erfahrungen. Der erste Bericht dieser Art ist bis zum … [54 Monate nach Inkrafttreten dieser Richtlinie] vorzulegen.

Artikel 36

[...]

[...]

[...]

Artikel 37

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.

Artikel 38

Umsetzung

(1) Die Mitgliedstaaten erlassen und veröffentlichen spätestens am … [...] **24** Monate nach dem Tag des Inkrafttretens dieser Richtlinie die Rechts- und Verwaltungsvorschriften, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis. Sie wenden diese Vorschriften ab dem... [einen Tag nach dem im ersten Unterabsatz genannten Datum] an.

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

Artikel 39

Änderung der Verordnung (EU) Nr. 910/2014

In der Richtlinie (EU) 910/2014 wird Artikel 19 [...] **mit Wirkung vom … [Datum der Frist für die Umsetzung der Richtlinie]** gestrichen.

Artikel 40

Änderung der Richtlinie (EU) 2018/1972

In der Richtlinie (EU) 2018/1972 werden die Artikel 40 und 41 [...] **mit Wirkung vom … [Datum der Frist für die Umsetzung der Richtlinie]** gestrichen.

Artikel 41

Aufhebung

Die Richtlinie (EU) 2016/1148 wird mit Wirkung vom ... [Datum der Frist für die Umsetzung der Richtlinie] aufgehoben.

Bezugnahmen auf die Richtlinie (EU) 2016/1148 gelten als Bezugnahmen auf die vorliegende Richtlinie und sind nach Maßgabe der Entsprechungstabelle in Anhang **II** [...] zu lesen.

Artikel 42

Inkrafttreten

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

Artikel 43

Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Brüssel am […]

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*

ANHANG I

SEKTOREN, TEILSEKTOREN UND ARTEN VON EINRICHTUNGEN

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 ([39]), die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 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 ([40])
		— Elektrizitätsmarktteilnehmer 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

[39] 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).

[40] Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54).

	b) Fernwärme und -kälte	— Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen ([41])
	c) Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		— zentrale Erdölbevorratungsstellen im Sinne des Artikels 2 Buchstabe f der Richtlinie 2009/119/EG des Rates ([42])
	d) Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG ([43])
		— 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

[41] 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).

[42] 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).

[43] 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).

		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
2. Verkehr	a) Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 ([44]), **die für gewerbliche Zwecke genutzt werden**
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG ([45]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 ([46]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		— Betreiber von Verkehrsmanagement- und

[44] 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).

[45] 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).

[46] 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).

		Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 ([47]) bereitstellen
	b) Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU ([48])
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 der Richtlinie 2012/34/EU
	c) Schifffahrt	— Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 ([49]) 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 ([50]), 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

[47] 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).

[48] 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).

[49] 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).

[50] 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).

		— Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG ([51])
	d) Straßenverkehr	— Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ([52]), die für Verkehrsmanagement- und Verkehrssteuerung verantwortlich sind, **ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme nur ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit sind**
		— Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU ([53])
3. Bankwesen		— Kreditinstitute im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 ([54]) **[, unter Ausschluss der in Artikel 2 Absatz 5 Nummer 8 genannten Kreditinstitute, die gemäß Artikel 2 Absatz 4 der Verordnung XX [DORA] ausgenommen sind]**

51 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).

52 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).

53 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).

54 Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 176 vom 27.6.2013, S. 1).

4. Finanzmarktinfrastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU ([55])
		— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 ([56])
5. Gesundheitswesen		— Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU ([57])
		— EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung XXXX/XXXX zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren[58]
		— Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG ([59]) 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

55 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).

56 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).

57 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).

58 [Verordnung des Europäischen Parlaments und des Rates zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU, Angabe zu aktualisieren nachdem der Vorschlag COM(2020) 727 final angenommen wurde].

59 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).

		Artikels 20 der Verordnung XXXX ([60]) („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 98/83/EG des Rates ([61]), jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch nur ein **nicht wesentlicher** Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist, die nicht als wesentliche oder wichtige Dienste eingestuft werden
7. Abwasser		Unternehmen, die kommunales, häusliches oder industrielles Abwasser im Sinne des Artikels 2 Nummern 1 bis 3 der Richtlinie 91/271/EWG des Rates ([62]) sammeln, entsorgen oder behandeln**, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung und die Behandlung solchen Abwassers nur 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-

60 [Verordnung des Europäischen Parlaments und des Rates zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und dem Krisenmanagement in Bezug auf Arzneimittel und Medizinprodukte; Angabe zu aktualisieren nachdem der Vorschlag COM(2020) 725 final angenommen wurde].

61 Richtlinie 98/83/EG des Rates vom 3. November 1998 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 330 vom 5.12.1998, S. 32).

62 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).

		Diensten
		— Anbieter von Rechenzentrumsdiensten
		— Betreiber von Inhaltszustellnetzen
		— Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) Nr. 910/2014 ([63])
		— Anbieter öffentlicher elektronischer Kommunikationsnetze im Sinne des Artikels 2 Nummer 8 der Richtlinie (EU) 2018/1972 ([64]) oder Anbieter elektronischer Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972 soweit deren Dienste öffentlich zugänglich sind
8.a Verwaltung von IKT-Diensten **(B2B)**		— **Anbieter verwalteter Dienste** — **Anbieter verwalteter Sicherheitsdienste**

63 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).

64 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).

9. **Einrichtungen der ö**ffentlichen Verwaltung		— Einrichtungen der öffentlichen Verwaltung von Zentralregierungen **entsprechend der Definition eines Mitgliedstaat gemäß nationalem Recht** — [...][65][...] — [...]
10. 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 im Sinne des Artikels 2 Nummer 8 der Richtlinie (EU) 2018/1972

65 [...]

ANHANG II

SEKTOREN, TEILSEKTOREN UND ARTEN VON EINRICHTUNGEN

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten im Sinne des Artikels 2 Nummer 1 der Richtlinie 97/67/EG ([66]), **einschließlich** [...] Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG ([67]), jedoch unter Ausschluss der Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist

66 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)**, geändert durch die Richtlinie 2008/6/EG des Europäischen Parlaments und des Rates vom 20. Februar 2008 zur Änderung der Richtlinie 97/67/EG im Hinblick auf die Vollendung des Binnenmarktes der Postdienste der Gemeinschaft (ABl. L 52 vom 27.2.2008, S. 3)**.

67 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).

3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne des Artikels 3 Nummern [...] 9 und 14 der Verordnung (EG) Nr. 1907/2006 ([68]), die Stoffe und **Gemische** [...] herstellen und mit diesen handeln**, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 dieser 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 ([69])**, die im Großhandel und 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 ([70]) herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 ([71]) herstellen, mit Ausnahme der unter Anhang I Nummer 5 aufgeführten Einrichtungen,

68 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).

69 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).

70 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).

71 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).

		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