# Amtsblatt der Europäischen Union

L 333

Ausgabe in deutscher Sprache

Rechtsvorschriften

65. Jahrgang

27. Dezember 2022


Inhalt


I *Gesetzgebungsakte*

VERORDNUNGEN

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

RICHTLINIEN

★ **Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)** [1] ..... 80

★ **Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor** [1] ..... 153

★ **Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates** [1] ..... 164


[1] Text von Bedeutung für den EWR.

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

I

*(Gesetzgebungsakte)*

# VERORDNUNGEN

## VERORDNUNG (EU) 2022/2554 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

**vom 14. Dezember 2022**

**über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011**

**(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 Kommission,

nach Übermittlung des Entwurfs des Gesetzgebungsaktes an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Informations- und Kommunikationstechnologien (IKT) unterstützen im digitalen Zeitalter komplexe Systeme, die für alltägliche Aktivitäten eingesetzt werden. Sie sorgen dafür, dass Schlüsselsektoren unserer Volkswirtschaften, einschließlich des Finanzsektors, am Laufen gehalten werden, und verbessern das Funktionieren des Binnenmarkts. Die zunehmende Digitalisierung und Vernetzung verstärken auch das IKT-Risiko, das die Gesellschaft insgesamt — und insbesondere das Finanzsystem — anfälliger für Cyberbedrohungen oder IKT-Störungen macht. Während die allgegenwärtige Nutzung von IKT-Systemen und die hohe Digitalisierung und Konnektivität heute grundlegende Merkmale der Tätigkeiten von Finanzunternehmen der Union sind, muss ihre digitale Resilienz erst noch besser angegangen und in ihre allgemeinen operativen Rahmen integriert werden.

(2) Die Nutzung von IKT hat in den letzten Jahrzehnten einen derart zentralen Stellenwert bei der Erbringung von Finanzdienstleistungen erlangt, dass sie heute entscheidend zur Ausführung typischer alltäglicher Aufgaben aller Finanzunternehmen beiträgt. Auf Digitalisierung beruhen heute beispielsweise Zahlungen, die von bargeld- und papiergestützten Methoden zunehmend auf die Nutzung digitaler Lösungen verlagert wurden, sowie Wertpapierclearing und -abrechnungssysteme, elektronischer und algorithmischer Handel, Darlehens- und Finanzierungsgeschäfte, Peer-to-Peer-Finanzierung, Bonitätseinstufung, Schadensmanagement und Back-Office-

([1]) ABl. C 343 vom 26.8.2021, S. 1.
([2]) ABl. C 155 vom 30.4.2021, S. 38.
([3]) Standpunkt des Europäischen Parlaments 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.

Transaktionen. Auch der Versicherungssektor hat sich durch den Einsatz von IKT verändert — vom Aufkommen digitaler Versicherungsvermittler, die ihre Dienste online anbieten und mit InsurTech arbeiten, bis hin zu digitalen Versicherungsgeschäften. Das Finanzwesen ist nicht nur sektorweit weitgehend digital geworden, sondern die Digitalisierung hat auch die Verflechtungen und Abhängigkeiten innerhalb des Finanzsektors sowie von Infrastrukturen Dritter und Drittdienstleistern verstärkt.

(3) Der Europäische Ausschuss für Systemrisiken (ESRB) bekräftigte in einem Bericht aus dem Jahr 2020 über systemische Cyberrisiken, wie das bestehende hohe Maß an Verflechtungen zwischen Finanzunternehmen, Finanzmärkten und Finanzmarktinfrastrukturen und insbesondere die gegenseitigen Abhängigkeiten ihrer IKT-Systeme eine Systemanfälligkeit herbeiführen könnten, da lokalisierte Cybervorfälle in einem der rund 22 000 Finanzunternehmen der Union über geografische Grenzen hinweg rasch auf das gesamte Finanzsystem übergreifen könnten. Schwerwiegende IKT-Sicherheitsverletzungen, die im Finanzsektor auftreten können, betreffen nicht nur Finanzunternehmen, die isoliert betrachtet werden. Ebenso können sich hierdurch ermittelte Schwachstellen über die Übertragungskanäle des Finanzsystems verbreiten und die Stabilität des Finanzsystems der Union beeinträchtigen, etwa durch Liquiditätsengpässe und einen allgemeinen Verlust des Vertrauens in die Finanzmärkte.

(4) Politische Entscheidungsträger, Regulierungsbehörden und Normungsgremien auf internationaler Ebene, Unionsebene und nationaler Ebene haben sich in den letzten Jahren mit dem IKT-Risiko befasst, um die digitale Resilienz zu stärken, Standards festzulegen und die Regulierungs- und Aufsichtsarbeit zu koordinieren. Auf internationaler Ebene sind der Basler Ausschuss für Bankenaufsicht, der Ausschuss für Zahlungsverkehr und Marktinfrastrukturen, der Rat für Finanzstabilität, das Institut für Finanzstabilität sowie die G7 und G20 bestrebt, den zuständigen Behörden und Marktteilnehmern in verschiedenen Rechtsordnungen Instrumente an die Hand zu geben, um die Resilienz ihrer Finanzsysteme zu stärken. Diesen Arbeiten lag auch die Notwendigkeit zugrunde, das IKT-Risiko im Kontext eines stark vernetzten globalen Finanzsystems zu berücksichtigen und sich um mehr Kohärenz der relevanten bewährten Verfahren zu bemühen.

(5) Das IKT-Risiko bleibt trotz gezielter politischer und legislativer Initiativen auf Unionsebene und nationaler Ebene eine Herausforderung für die operationale Resilienz, Leistungsfähigkeit und Stabilität des Finanzsystems der Union. Mit den Reformen nach der Finanzkrise von 2008 wurde in erster Linie die finanzielle Resilienz des Finanzsektors der Union gestärkt und darauf abgezielt, die Wettbewerbsfähigkeit und Stabilität der Union aus wirtschaftlicher, aufsichtsrechtlicher und marktpolitischer Sicht zu bewahren. Obwohl IKT-Sicherheit und digitale Resilienz Bestandteil des operationellen Risikos sind, standen sie in der Zeit nach der Finanzkrise weniger im Fokus der Regulierungsagenda und wurden nur in einigen Bereichen der Unionspolitik für Finanzdienstleistungen und Regulierung oder nur in wenigen Mitgliedstaaten weiterentwickelt.

(6) In ihrer Mitteilung mit dem Titel „FinTech-Aktionsplan: für einen wettbewerbsfähigeren und innovativen europäischen Finanzsektor“ vom 8. März 2018 hob die Kommission hervor, wie überaus wichtig es ist, den Finanzsektor der Union widerstandsfähiger zu machen, auch aus operativer Sicht, um seine technologische Sicherheit und sein reibungsloses Funktionieren sowie seine rasche Wiederherstellung nach IKT-Sicherheitsverletzungen und -Vorfällen zu gewährleisten, damit Finanzdienstleistungen in der gesamten Union — auch in Stresssituationen — wirksam und reibungslos erbracht werden können und gleichzeitig das Vertrauen der Verbraucher und der Märkte gewahrt wird.

(7) Im April 2019 veröffentlichten die mit der Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([4]) eingerichtete Europäische Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde, EBA), die mit der Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates ([5]) eingerichtete Europäische Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung,

([4]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

([5]) Verordnung (EU) Nr. 1094/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/79/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 48).

EIOPA) und die mit der Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates ([6]) eingerichtete Europäische Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde, ESMA) (zusammen als „Europäische Aufsichtsbehörden" oder „ESA", im Folgenden „ESA") gemeinsam fachliche Gutachten, in denen ein kohärenter Ansatz für das IKT-Risiko im Finanzbereich gefordert und empfohlen wurde, die digitale operationale Resilienz der Finanzdienstleistungsbranche durch eine sektorspezifische Initiative der Union auf verhältnismäßige Weise zu stärken.

(8) Der Finanzsektor der Union wird durch ein einheitliches Regelwerk (Single Rulebook) reguliert und unterliegt einem europäischen Finanzaufsichtssystem. Dennoch wurden Bestimmungen über die digitale operationale Resilienz und die IKT-Sicherheit noch nicht vollständig oder konsequent harmonisiert, obwohl die digitale operationale Resilienz für die Gewährleistung von Finanzstabilität und Marktintegrität im digitalen Zeitalter von entscheidender Bedeutung und nicht weniger wichtig ist als beispielsweise gemeinsame Aufsichts- oder Marktverhaltensstandards. Daher sollten das einheitliche Regelwerk und das Aufsichtssystem so weiterentwickelt werden, dass sie auch die digitale operationale Resilienz abdecken, indem die Mandate der zuständigen Behörden gestärkt werden, damit sie zur Wahrung der Integrität und der Effizienz des Binnenmarkts und zur Förderung seines ordnungsgemäßen Funktionierens des Managements des IKT-Risikos im Finanzsektor überwachen können.

(9) Rechtliche Unterschiede und ungleiche nationale Regulierungs- oder Aufsichtsansätze in Bezug auf das IKT-Risiko schaffen Hindernisse für das Funktionieren des Binnenmarkts für Finanzdienstleistungen und erschweren grenzüberschreitend tätigen Finanzunternehmen die reibungslose Ausübung der Niederlassungsfreiheit und die Erbringung von Dienstleistungen. Auch der Wettbewerb zwischen denselben Arten von Finanzunternehmen, die in verschiedenen Mitgliedstaaten tätig sind, könnte verzerrt werden. Dies gilt insbesondere in Bereichen, in denen die Harmonisierung auf Unionsebene bislang sehr begrenzt — wie beim Testen der digitalen operationalen Resilienz — oder gar nicht vorhanden ist — wie bei der Überwachung des IKT-Drittparteienrisikos. Unterschiede, die sich aus den auf nationaler Ebene geplanten Entwicklungen ergeben, könnten weitere Hindernisse für das Funktionieren des Binnenmarkts schaffen, die sich nachteilig auf die Marktteilnehmer und die Finanzstabilität auswirken.

(10) Da die einschlägigen Bestimmungen über IKT-Risiken bisher auf Unionsebene nur auf unvollständige Art und Weise angegangen wurden, bestehen Lücken oder Überschneidungen in wichtigen Bereichen — wie der Meldung IKT-bezogener Vorfälle und Tests der digitalen operationalen Resilienz — sowie Unstimmigkeiten aufgrund sich abzeichnender unterschiedlicher nationaler Vorschriften oder einer kostenineffizienten Anwendung sich überschneidender Vorschriften. Dies ist besonders schädlich für intensive IKT-Nutzer wie den Finanzsektor, da technologische Risiken keine Grenzen haben und der Finanzsektor seine Dienste auf breiter grenzüberschreitender Basis inner- und außerhalb der Union erbringt. Einzelne Finanzunternehmen, die grenzüberschreitend tätig sind oder über mehrere Zulassungen verfügen (z. B. kann ein Finanzunternehmen eine Lizenz für eine Bank, eine Wertpapierfirma und ein Zahlungsinstitut besitzen, die jeweils von einer anderen zuständigen Behörde in einem oder mehreren Mitgliedstaaten ausgestellt wurde), stehen bei der alleinigen und kohärenten und kostenwirksamen Bewältigung des IKT-Risikos und der Abmilderung nachteiliger Auswirkungen von IKT-Vorfällen vor operativen Herausforderungen.

(11) Da das einheitliche Regelwerk nicht mit einem umfassenden Rahmen für IKT oder operationelle Risiken einhergeht, ist eine weitere Harmonisierung der wichtigsten Anforderungen an die digitale operationale Resilienz für alle Finanzunternehmen erforderlich. Die Entwicklung der IKT-Kapazitäten und der allgemeinen Resilienz durch Finanzunternehmen auf der Grundlage dieser Kernanforderungen, um operativen Ausfällen standzuhalten, würde dabei helfen, die Stabilität und Integrität der Finanzmärkte der Union zu erhalten, und auf diese Weise dazu beitragen, ein hohes Schutzniveau für Anleger und Verbraucher in der Union sicherzustellen. Da diese Verordnung zum reibungslosen Funktionieren des Binnenmarkts beitragen soll, sollte sie sich auf die Bestimmungen von Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) in der Auslegung der ständigen Rechtsprechung des Gerichtshofs der Europäischen Union (im Folgenden „Gerichtshof") stützen.

(12) Mit dieser Verordnung sollen die Anforderungen mit Blick auf IKT-Risiken im Rahmen der Anforderungen an das operationelle Risiko konsolidiert und verbessert werden, die bisher in verschiedenen Rechtsakten der Union gesondert behandelt wurden. Diese Rechtsakte deckten zwar die wichtigsten Kategorien finanzieller Risiken ab (z. B. Kreditrisiko, Marktrisiko, Gegenparteiausfallrisiko, Liquiditätsrisiko und Marktrisiko), waren aber bei ihrer Annahme nicht umfassend auf alle Komponenten der operationalen Resilienz ausgerichtet. Bei der Weiterentwicklung der Vorschriften über das operationelle Risiko in diesen Rechtsakten der Union wurde häufig ein traditioneller quantitativer Ansatz zur Bewältigung von Risiken (d. h. die Festlegung einer Kapitalvorgabe zur Absicherung gegen

([6]) Verordnung (EU) Nr. 1095/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Wertpapier- und Marktaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/77/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 84).

das IKT-Risiko) bevorzugt, anstelle gezielter qualitativer Vorschriften für den Schutz, die Erkennung, Eindämmung, Wiederherstellung und die Sanierungskapazitäten bei IKT-bezogenen Vorfällen oder für die Kapazitäten für Meldungen und Tests digitaler Technologie. Mit diesen Rechtsakten sollten in erster Linie wesentliche Vorschriften über die Beaufsichtigung, die Integrität oder das Verhalten des Marktes abgedeckt und aktualisiert werden. Indem die verschiedenen Vorschriften über IKT-Risiken konsolidiert und verbessert werden, sollten alle Bestimmungen, die sich mit digitalen Risiken im Finanzsektor befassen, erstmals in einheitlicher Weise in einem einzigen Rechtsakt zusammengefasst werden. Somit schließt diese Verordnung Lücken oder behebt Unstimmigkeiten in einigen der vorausgehenden Rechtsakte (auch in Bezug auf die darin verwendete Terminologie) und nimmt durch gezielte Vorschriften über die Kapazitäten für das IKT-Risikomanagement, die Meldung von Vorfällen, Tests der operationalen Resilienz sowie die Überwachung des IKT-Drittparteienrisikos ausdrücklich auf IKT-Risiken Bezug. Somit sollte diese Verordnung auch für das IKT-Risiko sensibilisieren und berücksichtigen, dass die finanzielle Solidität von Finanzunternehmen durch IKT-Vorfälle und eine mangelnde operationale Resilienz beeinträchtigt werden könnten.

(13) Finanzunternehmen sollten bei der Bewältigung von IKT-Risiken denselben Ansatz und dieselben grundsatzbasierten Regeln befolgen, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist. Kohärenz trägt dazu bei, das Vertrauen in das Finanzsystem zu stärken und dessen Stabilität zu erhalten, insbesondere in Zeiten starker Abhängigkeit von IKT-Systemen, -Plattformen und -Infrastrukturen, die erhöhtes digitales Risiko mit sich bringt. Ebenso sollte durch Einhaltung einer grundlegenden Cyberhygiene verhindert werden, dass der Wirtschaft durch die Minimierung der Auswirkungen und Kosten von IKT-Störfällen hohe Kosten entstehen.

(14) Eine Verordnung hilft, die Komplexität der Regulierung zu verringern, fördert die aufsichtliche Konvergenz, erhöht die Rechtssicherheit und trägt ferner dazu bei, die Befolgungskosten, insbesondere für grenzüberschreitend tätige Finanzunternehmen, zu begrenzen und Wettbewerbsverzerrungen zu verringern. Daher ist die Wahl einer Verordnung zur Schaffung eines gemeinsamen Rahmens für die digitale operationale Resilienz von Finanzunternehmen am besten geeignet, eine einheitliche und kohärente Anwendung aller Komponenten des IKT-Risikomanagements im Finanzsektor der Union zu gewährleisten.

(15) Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([7]) stellte den ersten horizontalen Rahmen für die Cybersicherheit auf Unionsebene dar, der auch für drei Arten von Finanzunternehmen, namentlich für Kreditinstitute, Handelsplätze und zentrale Gegenparteien gilt. Da in der Richtlinie (EU) 2016/1148 jedoch ein Mechanismus zur Identifizierung der Betreiber wesentlicher Dienste auf nationaler Ebene vorgesehen ist, wurden nur bestimmte Kreditinstitute, Handelsplätze und zentrale Gegenparteien, die von den Mitgliedstaaten ermittelt wurden, in der Praxis in den Anwendungsbereich der Richtlinie aufgenommen und daher verpflichtet, die darin festgelegten Anforderungen an die IKT-Sicherheit und die Meldung von Vorfällen zu erfüllen. Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([8]) legt ein einheitliches Kriterium dafür fest, welche Unternehmen in ihren Anwendungsbereich fallen (Schwellenwert für die Größe), wobei auch die drei Arten von Finanzunternehmen in ihrem Anwendungsbereich verbleiben.

(16) Da mit dieser Verordnung jedoch das Ausmaß der Harmonisierung in Bezug auf die verschiedenen Komponenten der digitalen Resilienz erhöht wird, indem Anforderungen an das IKT-Risikomanagement und die Meldung von IKT-Vorfällen eingeführt werden, die strenger sind als diejenigen im aktuellen Finanzdienstleistungsrecht der Union, stellt dies auch im Vergleich zu den Anforderungen der Richtlinie (EU) 2022/2555 eine stärkere Harmonisierung dar. Folglich verkörpert diese Verordnung eine *Lex specialis* zur Richtlinie (EU) 2022/2555. Es ist zugleich von entscheidender Bedeutung, dass eine enge Beziehung zwischen dem Finanzsektor und dem derzeit in der Richtlinie (EU) 2022/2555 festgelegten horizontalen Rahmen der Union für Cybersicherheit aufrechterhalten wird, um die Kohärenz mit den von den Mitgliedstaaten angenommenen Strategien für Cybersicherheit zu gewährleisten und es Finanzaufsichtsbehörden zu ermöglichen, auf Cybervorfälle aufmerksam gemacht zu werden, die andere unter die genannte Richtlinie fallende Sektoren betreffen.

([7]) 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).

([8]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (siehe Seite 80 dieses Amtsblatts).

(17) Im Einklang mit Artikel 4 Absatz 2 des Vertrags über die Europäische Union und unbeschadet der gerichtlichen Überprüfung durch den Gerichtshof sollte diese Verordnung die Zuständigkeit der Mitgliedstaaten für die grundlegenden Funktionen des Staates in Bezug auf die öffentliche Sicherheit, die Verteidigung und den Schutz der nationalen Sicherheit — z. B. in Bezug auf die Bereitstellung von Informationen, die dem Schutz der nationalen Sicherheit zuwiderlaufen würden — unberührt lassen.

(18) Um sektorübergreifendes Lernen zu ermöglichen und Erfahrungen anderer Sektoren beim Umgang mit Cyberbedrohungen wirksam zu nutzen, sollten Finanzunternehmen im Sinne der Richtlinie (EU) 2022/2555 Teil des „Ökosystems" jener Richtlinie bleiben (z. B. Kooperationsgruppe und Computer-Notfallteam (computer security incident response team, CSIRT)). Die ESA und zuständige nationale Behörden sollten in der Lage sein, sich an den strategischen politischen Diskussionen und der technischen Arbeit der Kooperationsgruppe im Sinne der genannten Richtlinie zu beteiligen, Informationen austauschen und mit den entsprechend der genannten Richtlinie benannten oder eingerichteten zentralen Anlaufstellen weiter zusammenarbeiten. Die nach der vorliegenden Verordnung zuständigen Behörden sollten auch die CSIRT konsultieren und mit ihnen zusammenarbeiten. Darüber hinaus sollten die zuständigen Behörden die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden um fachliche Beratung ersuchen und Kooperationsvereinbarungen schließen können, mit denen wirksame und schnelle Koordinierungsmechanismen sichergestellt werden sollen.

(19) Angesichts der engen Verflechtungen zwischen der digitalen Resilienz und der physischen Resilienz von Finanzunternehmen ist in der vorliegenden Verordnung und in der Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates ([9]) ein kohärenter Ansatz in Bezug auf die Resilienz kritischer Einrichtungen erforderlich. Da das IKT-Risikomanagement und die Meldepflichten nach der vorliegenden Verordnung der physischen Resilienz von Finanzunternehmen umfassend Rechnung tragen, sollten die in den Kapiteln III und IV der Richtlinie (EU) 2022/2557 festgelegten Verpflichtungen nicht für Finanzunternehmen gelten, die in den Anwendungsbereich der genannten Richtlinie fallen.

(20) Anbieter von Cloud-Computing-Diensten sind eine Kategorie digitaler Infrastruktur, die unter die Richtlinie (EU) 2022/2555 fällt. Der mit dieser Verordnung geschaffene Überwachungsrahmen der Union (im Folgenden „Überwachungsrahmen") gilt für alle kritischen IKT-Drittdienstleister, einschließlich Anbietern von Cloud-Computing-Diensten, die Finanzunternehmen IKT-Dienstleistungen bereitstellen, und sollte als Ergänzung zu der Beaufsichtigung gemäß der Richtlinie (EU) 2022/2555 betrachtet werden. Darüber hinaus sollte der mit dieser Verordnung geschaffene Überwachungsrahmen für Anbieter von Cloud-Computing-Diensten gelten, wenn es keinen horizontalen Rahmen der Union gibt, mit dem eine Behörde für die digitale Überwachung eingerichtet wird.

(21) Um die vollständige Kontrolle über das IKT-Risiko zu behalten, müssen Finanzunternehmen über umfassende Kapazitäten verfügen, die ein leistungsfähiges und wirksames IKT-Risikomanagement sowie spezifische Mechanismen und Strategien für die Handhabung aller IKT-bezogener Vorfälle und für die Meldung schwerwiegender IKT-bezogener Vorfälle ermöglichen. Ebenso sollten Finanzunternehmen über Leit- und Richtlinien für die Erprobung von IKT-Systemen, -Kontrollen und -Prozessen sowie für das Management des IKT-Drittparteienrisikos verfügen. Die Mindestanforderungen an die digitale operationale Resilienz für Finanzunternehmen sollten angehoben werden, wobei auch eine verhältnismäßige Anwendung der Anforderungen für bestimmte Finanzunternehmen möglich sein sollte, insbesondere bei Kleinstunternehmen sowie Finanzunternehmen, die einem vereinfachten IKT-Risikomanagementrahmen unterliegen. Um eine effiziente Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung zu ermöglichen, die verhältnismäßig ist und der Notwendigkeit Rechnung trägt, den Verwaltungsaufwand für die zuständigen Behörden zu verringern, sollten die einschlägigen nationalen Aufsichtsmechanismen für derartige Finanzunternehmen deren Größe und Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigen, auch wenn die in Artikel 5 der Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates ([10]) festgelegten einschlägigen Schwellenwerte überschritten werden. Insbesondere sollten sich die Aufsichtstätigkeiten vorrangig auf die Notwendigkeit konzentrieren, ernsthaften Risiken im Zusammenhang mit dem IKT-Risikomanagement eines bestimmten Unternehmens entgegenzuwirken.

([9]) Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates (siehe Seite 164 dieses Amtsblatts).

([10]) Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates vom 14. Dezember 2016 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (EbAV) (ABl. L 354 vom 23.12.2016, S. 37).

Die zuständigen Behörden sollten auch einen wachsamen, aber verhältnismäßigen Ansatz in Bezug auf die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung verfolgen, die gemäß Artikel 31 der Richtlinie (EU) 2016/2341 einen wesentlichen Teil ihres Kerngeschäfts, wie Vermögensverwaltung, versicherungsmathematische Berechnungen, Rechnungslegung und Datenverwaltung, an Dienstleister auslagern.

(22) Die Schwellenwerte und Taxonomien für die Meldung IKT-bezogener Vorfälle unterscheiden sich auf nationaler Ebene erheblich. Wenngleich sich durch einschlägige Arbeiten der durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates ([11]) eingerichtete Agentur der Europäischen Union für Cybersicherheit (ENISA) und der Kooperationsgruppe im Sinne der Richtlinie (EU) 2022/2555 eine gemeinsame Grundlage schaffen lässt, bestehen für die übrigen Finanzunternehmen noch immer unterschiedliche Ansätze in Bezug auf die Festlegung der Schwellenwerte und die Verwendung von Taxonomien bzw. können sich für diese ergeben. Aufgrund dieser Unterschiede besteht eine Vielzahl von Anforderungen, die Finanzunternehmen einhalten müssen, insbesondere wenn sie in mehreren Mitgliedstaaten tätig sind und Teil einer Finanzgruppe sind. Darüber hinaus können derartige Unterschiede die Einrichtung weiterer einheitlicher oder zentralisierter Mechanismen der Union behindern, die das Meldeverfahren beschleunigen und einen raschen und reibungslosen Informationsaustausch zwischen den zuständigen Behörden unterstützen, was für die Bewältigung des IKT-Risikos bei Großangriffen mit potenziell systemischen Folgen von entscheidender Bedeutung ist.

(23) Um für bestimmte Finanzunternehmen den Verwaltungsaufwand zu verringern und potenziell doppelte Meldepflichten zu vermeiden, sollte die Verpflichtung zur Meldung von Vorfällen gemäß der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates ([12]) nicht mehr für Zahlungsdienstleister gelten, die in den Geltungsbereich dieser Verordnung fallen. Folglich sollten Kreditinstitute, E-Geld-Institute, Zahlungsinstitute und Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der genannten Richtlinie alle zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle, die vormals gemäß der genannten Richtlinie gemeldet wurden, ab dem Geltungsbeginn dieser Verordnung gemäß dieser melden, und zwar unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht.

(24) Um den zuständigen Behörden die Erfüllung von Aufsichtsaufgaben zu ermöglichen, indem sie einen vollständigen Überblick über Art, Häufigkeit, Ausmaß und Auswirkungen IKT-bezogener Vorfälle erhalten, und um den Informationsaustausch zwischen einschlägigen Behörden, einschließlich Strafverfolgungs- und Abwicklungsbehörden, zu verbessern, sollte diese Verordnung eine solide Regelung für die Meldung IKT-bezogener Vorfälle festlegen, wobei die einschlägigen Anforderungen derzeitige Lücken im Finanzdienstleistungsrecht schließen, und Überschneidungen und Doppelarbeit mit Blick auf eine Senkung der Kosten beseitigen. Es ist von entscheidender Bedeutung, die Regelung für die Meldung IKT-bezogener Vorfälle zu harmonisieren, indem alle Finanzunternehmen verpflichtet werden, ihren zuständigen Behörden in dem in dieser Verordnung vorgesehenen einheitlichen, gestrafften Rahmen Bericht zu erstatten. Darüber hinaus sollten die ESA ermächtigt werden, relevante Aspekte für den Rahmen für die Meldung IKT-bezogener Vorfälle — wie Taxonomie, Zeitrahmen, Datensätze, Vorlagen und anwendbare Schwellenwerte — näher zu spezifizieren. Um vollständige Übereinstimmung mit der Richtlinie (EU) 2022/2555 zu gewährleisten, sollten Finanzunternehmen der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden können, wenn sie der Auffassung sind, dass die Cyberbedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist.

(25) In einigen Teilsektoren des Finanzsektors wurden Anforderungen für Tests der digitalen operationalen Resilienz entwickelt, deren Rahmen nicht immer vollständig aneinander angeglichen waren. Dies führt zu potenziell doppelten Kosten für grenzüberschreitend tätige Finanzunternehmen und verkompliziert die gegenseitige Anerkennung der Ergebnisse von Tests der digitalen operationalen Resilienz, was wiederum zu einer Fragmentierung des Binnenmarkts führen könnte.

([11]) 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).

([12]) Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

(26) Darüber hinaus bleiben Schwachstellen, wenn keine IKT-Tests vorgeschrieben sind, unentdeckt, wodurch ein Finanzunternehmen IKT-Risiken ausgesetzt wird und letztlich ein höheres Risiko für die Stabilität und Integrität des Finanzsektors entsteht. Ohne ein Tätigwerden der Union wären Tests der digitalen operationalen Resilienz weiterhin uneinheitlich, und es gäbe kein System für die gegenseitige Anerkennung der IKT-Testergebnisse in verschiedenen Rechtsordnungen. Da es unwahrscheinlich ist, dass Testregelungen in anderen Teilsektoren des Finanzsektors in bedeutendem Umfang eingeführt würden, gingen darüber hinaus die potenziellen Vorteile eines Rahmens für Tests im Hinblick auf die Aufdeckung von Schwachstellen und Risiken sowie von Tests von Verteidigungsfähigkeiten und die Fortführung der Geschäftstätigkeit verloren, die zur Stärkung des Vertrauens von Kunden, Lieferanten und Geschäftspartnern beitragen. Um diese Überschneidungen, Divergenzen und Lücken zu beseitigen, müssen Vorschriften für ein koordiniertes Testsystem festgelegt werden, damit die gegenseitige Anerkennung erweiterter Tests für diejenigen Finanzunternehmen erleichtert wird, die die Kriterien in dieser Verordnung erfüllen.

(27) Die Abhängigkeit der Finanzunternehmen von IKT-Dienstleistungen ist zum Teil darauf zurückzuführen, dass sie sich an eine sich entwickelnde wettbewerbsorientierte digitale Weltwirtschaft anpassen, ihre geschäftliche Effizienz steigern und die Verbrauchernachfrage befriedigen müssen. Die Art und das Ausmaß dieser Nutzung von IKT-Dienstleistungen haben sich in den letzten Jahren ständig weiterentwickelt, was zu Kostensenkungen bei der Finanzintermediation geführt hat, die Expansion von Unternehmen und die Skalierbarkeit bei der Ausübung von Finanztätigkeiten ermöglicht und gleichzeitig ein breites Spektrum an IKT-Tools für die Verwaltung komplexer interner Prozesse zur Verfügung gestellt hat.

(28) Die umfangreiche Nutzung von IKT-Dienstleistungen zeigt sich an komplexen vertraglichen Vereinbarungen, wobei Finanzunternehmen häufig Schwierigkeiten haben, Vertragsbedingungen auszuhandeln, die auf die Aufsichtsstandards oder sonstige aufsichtsrechtliche Anforderungen, denen sie unterliegen, zugeschnitten sind; Gleiches gilt für die Durchsetzung bestimmter Rechte, wie Zugangs- oder Auditrechte, selbst wenn diese in ihren vertraglichen Vereinbarungen verankert sind. Darüber hinaus fehlen in vielen dieser vertraglichen Vereinbarungen ausreichende Garantien, die die vollständige Überwachung von Verfahren für die Unterauftragsvergabe ermöglichen, wodurch das Finanzunternehmen die damit verbundenen Risiken nicht bewerten kann. Da IKT-Drittdienstleister häufig standardisierte Dienstleistungen für verschiedene Arten von Kunden anbieten, wird den individuellen oder spezifischen Bedürfnissen der Akteure der Finanzbranche in derartigen vertraglichen Vereinbarungen nicht immer angemessen Rechnung getragen.

(29) Obwohl die Rechtsvorschriften für Finanzdienstleistungen bestimmte allgemeine Vorschriften über die Auslagerung von Tätigkeiten enthalten, ist die Überwachung der vertraglichen Dimension nicht vollständig in den Rechtsvorschriften der Union verankert. Weil eindeutige und angepasste Unionsstandards, die auf die vertraglichen Vereinbarungen mit IKT-Drittdienstleistern anwendbar sind, fehlen, werden externe Quellen für IKT-Risiken nicht umfassend behandelt. Daher müssen bestimmte Schlüsselprinzipien festgelegt werden, die Finanzunternehmen als Richtschnur für das Management des IKT-Drittparteienrisikos dienen und von besonderer Bedeutung sind, wenn Finanzunternehmen zur Unterstützung ihrer kritischen oder wichtigen Funktionen auf IKT-Drittdienstleister zurückgreifen. Diese Prinzipien sollten mit einer Reihe grundlegender vertraglicher Rechte einhergehen, die sich auf mehrere Aspekte bei der Erfüllung und Beendigung von vertraglichen Vereinbarungen beziehen, damit bestimmte Mindestgarantien geboten werden, um die Fähigkeit von Finanzunternehmen, alle von Drittdienstleistern ausgehenden IKT-Risiken wirksam zu überwachen, zu stärken. Diese Prinzipien ergänzen die für die Auslagerung geltenden sektorspezifischen Rechtsvorschriften.

(30) Ein gewisser Mangel an Homogenität und Konvergenz in Bezug auf die Überwachung des IKT-Drittparteienrisikos und die Abhängigkeit von IKT-Drittdienstleistern ist derzeit festzustellen. Obwohl Anstrengungen unternommen wurden, um den Bereich der Auslagerung anzugehen, wie beispielsweise die Leitlinien der EBA zu Auslagerung von 2019 und Leitlinien der ESMA zur Auslagerung an Cloud-Anbieter von 2021, wird die allgemeinere Frage der Eindämmung systemischer Risiken, die entstehen könnten, wenn der Finanzsektor einer begrenzten Anzahl kritischer IKT-Drittdienstleister ausgesetzt ist, im Unionsrecht nicht ausreichend behandelt. Der Mangel an Vorschriften auf Unionsebene wird noch dadurch verschärft, dass es keine nationalen Vorschriften für die Mandate und Instrumente gibt, die es Finanzaufsichtsbehörden ermöglichen, Abhängigkeiten von IKT-Drittdienstleistern ordnungsgemäß zu erfassen und Risiken, die sich aus der Konzentration der Abhängigkeiten von IKT-Drittdienstleistern ergeben, angemessen zu überwachen.

(31) Unter Berücksichtigung der potenziellen Systemrisiken, die mit der verstärkten Auslagerung und der Konzentration der Abhängigkeiten von IKT-Drittdienstleistern verbunden sind, und in Anbetracht nationaler Regelungen, die den Finanzaufsichtsbehörden unzureichend Werkzeuge bereitstellen, die geeignet sind, die Folgen der bei kritischen IKT-Drittdienstleistern auftretenden IKT-Risiken zu quantifizieren, zu qualifizieren und zu beheben, muss ein geeigneter Überwachungsrahmen geschaffen werden, der eine kontinuierliche Überwachung der Tätigkeiten von IKT-Drittdienstleistern, bei denen es sich um für Finanzunternehmen kritische IKT-Drittdienstleister handelt, ermöglicht und zugleich bei Kunden, bei denen es sich nicht um Finanzunternehmen handelt, Vertraulichkeit und Sicherheit gewährleistet. Auch wenn mit der gruppeninternen Bereitstellung von IKT-Dienstleistungen spezifische Risiken und Vorteile einhergehen, sollte sie nicht automatisch als weniger riskant angesehen werden als die Bereitstellung von IKT-Dienstleistungen durch Dienstleister außerhalb einer Finanzgruppe und sollte daher demselben Rechtsrahmen unterliegen. Wenn IKT-Dienstleistungen innerhalb einer Finanzgruppe bereitgestellt werden, könnten Finanzunternehmen möglicherweise jedoch ein höheres Maß an Kontrolle über gruppeninterne Dienstleister haben, was bei der Gesamtrisikobewertung berücksichtigt werden sollte.

(32) Da IKT- Risiken immer komplexer und technisch ausgereifter werden, hängen gute Maßnahmen für die Erkennung und Prävention von IKT-Risiken in hohem Maße von einem regelmäßigen Informationsaustausch zwischen Finanzunternehmen über Bedrohungen und Schwachstellen ab. Ein Informationsaustausch trägt dazu bei, das Bewusstsein für Cyberbedrohungen zu schärfen. Dies wiederum verstärkt die Fähigkeit der Finanzunternehmen, zu verhindern, dass Cyberbedrohungen in reale IKT-bezogene Vorfälle münden, und versetzt Finanzunternehmen in die Lage, die Auswirkungen IKT-bezogener Vorfälle wirksamer einzudämmen und sich schneller zu erholen. In Ermangelung von Leitlinien auf Unionsebene scheinen mehrere Faktoren einen solchen Wissensaustausch verhindert zu haben, darunter insbesondere die Unsicherheit hinsichtlich der Vereinbarkeit mit den Datenschutz-, Kartell- und Haftungsvorschriften.

(33) Darüber hinaus führen Zweifel bezüglich der Art von Informationen, die mit anderen Marktteilnehmern oder mit Nicht-Aufsichtsbehörden (z. B. ENISA für analytische Eingaben oder Europol für Strafverfolgungszwecke) ausgetauscht werden können, dazu, dass nützliche Informationen vorenthalten werden. Deswegen sind Umfang und Qualität des Informationsaustauschs derzeit nach wie vor begrenzt und fragmentiert, wobei der einschlägige Austausch hauptsächlich auf lokaler Ebene (über nationale Initiativen) erfolgt und keine einheitlichen unionsweiten Regelungen für den Informationsaustausch bestehen, die auf die Bedürfnisse eines integrierten Finanzsystems zugeschnitten sind. Aus diesem Grund ist es wichtig, diese Kommunikationskanäle zu stärken.

(34) Finanzunternehmen sollten ermutigt werden, Informationen und Erkenntnisse zu Cyberbedrohungen untereinander auszutauschen und 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, indem sie an Vereinbarungen über den Austausch von Informationen teilnehmen. Daher muss auf Unionsebene die Einrichtung von Regelungen für freiwillige Vereinbarungen über den Informationsaustausch ermöglicht werden, die — bei der Umsetzung in vertrauenswürdigen Umgebungen — der Finanzwelt dabei helfen würden, Cyberbedrohungen vorzubeugen und gemeinsam auf diese zu reagieren, indem die Ausbreitung von IKT-Risiken rasch eingedämmt und potenzielle Ansteckungseffekte über alle Finanzkanäle hinweg verhindert werden. Diese Regelungen sollten mit dem anwendbaren Wettbewerbsrecht der Union, das in der Mitteilung der Kommission vom 14. Januar 2011 mit dem Titel „Leitlinien zur Anwendbarkeit des Artikels 101 des Vertrags über die Arbeitsweise der Europäischen Union auf Vereinbarungen über horizontale Zusammenarbeit“ sowie den Datenschutzvorschriften der Union und insbesondere der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([13]) im Einklang stehen. Sie sollten auf der Grundlage einer oder mehrerer der in Artikel 6 jener Verordnung festgelegten Rechtsgrundlagen tätig werden, beispielsweise im Zusammenhang mit der Verarbeitung personenbezogener Daten, die zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten gemäß Artikel 6 Absatz 1 Buchstabe f jener Verordnung erforderlich ist, sowie im Zusammenhang mit der Verarbeitung personenbezogener Daten, die für die Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt, oder für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, gemäß Artikel 6 Absatz 1 Buchstabe c bzw. e jener Verordnung erforderlich ist.

([13]) 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).

(35) Um ein hohes Niveau an digitaler operationaler Resilienz im gesamten Finanzsektor aufrechtzuerhalten und zugleich mit den technologischen Entwicklungen Schritt zu halten, sollte in der vorliegenden Verordnung auf Risiken eingegangen werden, die sich aus allen Arten von IKT-Dienstleistungen ergeben. Zu diesem Zweck sollte die Definition von IKT-Dienstleistungen im Zusammenhang mit der vorliegenden Verordnung weit ausgelegt werden und digitale Dienste und Datendienste umfassen, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern fortlaufend bereitgestellt werden. Diese Definition sollte beispielsweise sogenannte „Over-the-top"-Dienste umfassen, die unter die Kategorie der elektronischen Kommunikationsdienste fallen. Sie sollte nur die begrenzte Kategorie traditioneller analoger Telefondienste ausschließen, die als Dienste des öffentlichen Fernsprechnetzes (PSTN — Public Switched Telephone Network), Festnetz-Dienste, herkömmliche Fernsprechdienste (POTS — Plain Old Telephone Service) oder Festnetztelefondienste gelten.

(36) Ungeachtet des in dieser Verordnung vorgesehenen breiten Geltungsbereichs sollten bei der Anwendung der Vorschriften für die digitale operationale Resilienz die wesentlichen Unterschiede zwischen Finanzunternehmen in Bezug auf deren Größe und Gesamtrisikoprofil berücksichtigt werden. Als Grundprinzip sollten Finanzunternehmen bei der Verteilung von Ressourcen und Kapazitäten für die Umsetzung des Rahmens für das IKT-Risikomanagement ihren IKT-Bedarf sorgfältig auf ihre Größe und ihr Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte abstimmen, während die zuständigen Behörden den Ansatz einer solchen Verteilung weiterhin bewerten und überprüfen sollten.

(37) Die in Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 genannten Kontoinformationsdienstleister werden unter Berücksichtigung der Besonderheiten ihrer Tätigkeiten und der mit ihnen verbundenen Risiken ausdrücklich in den Geltungsbereich der vorliegenden Verordnung einbezogen. Darüber hinaus fallen gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates ([14]) und Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 ausgenommene E-Geld-Institute und Zahlungsinstitute auch dann in den Geltungsbereich dieser Verordnung, wenn ihnen keine Zulassung gemäß der Richtlinie 2009/110/EG für die Ausgabe von E-Geld erteilt wurde oder wenn ihnen keine Zulassung für die Erbringung und Ausführung von Zahlungsdiensten gemäß der Richtlinie (EU) 2015/2366 erteilt wurde. Postscheckämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates ([15]) sind jedoch vom Geltungsbereich der vorliegenden Verordnung ausgenommen. Die zuständige Behörde für die nach der Richtlinie (EU) 2015/2366 ausgenommenen Zahlungsinstitute, die nach der Richtlinie 2009/110/EG ausgenommenen E-Geld-Institute und die Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 sollte die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde sein.

(38) Da größere Finanzunternehmen unter Umständen über umfangreichere Ressourcen verfügen und rasch Mittel für die Einrichtung von Governance-Strukturen und die Einführung verschiedener Unternehmensstrategien bereitstellen könnten, sollten nur Finanzunternehmen, die keine Kleinstunternehmen im Sinne dieser Verordnung sind, verpflichtet werden, komplexere Governance-Regelungen einzuführen. Diese Unternehmen sind besser gerüstet, um insbesondere spezielle Managementfunktionen für die Überwachung von Vereinbarungen mit IKT-Drittdienstleistern oder für den Umgang mit dem Krisenmanagement einzurichten, ihr IKT-Risikomanagement nach dem Modell der drei Verteidigungslinien zu strukturieren oder ein internes Modell für Risikomanagement und Kontrolle einzuführen und ihren IKT-Risikomanagementrahmen internen Revisionen zu unterziehen.

(39) Einige Finanzunternehmen kommen in den Genuss von Ausnahmen oder unterliegen gemäß dem einschlägigen sektorspezifischen Unionsrecht einem sehr lockeren Regelungsrahmen. Zu diesen Finanzunternehmen zählen Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates ([16]), Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates ([17]) und Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt nicht mehr als 15 Versorgungs-

([14]) Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG (ABl. L 267 vom 10.10.2009, S. 7).

([15]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([16]) Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010 (ABl. L 174 vom 1.7.2011, S. 1).

([17]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

anwärtern betreiben. Angesichts dieser Ausnahmen wäre es nicht verhältnismäßig, diese Finanzunternehmen in den Geltungsbereich der vorliegenden Verordnung aufzunehmen. Darüber hinaus wird in der vorliegenden Verordnung den strukturellen Besonderheiten des Versicherungsvermittlermarkts Rechnung getragen, sodass Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, die als Kleinstunternehmen oder als kleine oder mittlere Unternehmen gelten, nicht unter diese Verordnung fallen sollten.

(40) Da die in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU genannten Einrichtungen vom Anwendungsbereich jener Richtlinie ausgenommen sind, sollten die Mitgliedstaaten beschließen können, diejenigen dieser Einrichtungen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, von der Anwendung dieser Verordnung auszunehmen.

(41) Um diese Verordnung an den Anwendungsbereich der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([18]) anzugleichen, ist es auch angezeigt, diejenigen in Artikel 2 und 3 jener Richtlinie genannten natürlichen und juristischen Personen, die Wertpapierdienstleistungen erbringen dürfen, ohne eine Zulassung gemäß der genannten Richtlinie erhalten zu müssen, vom Geltungsbereich der vorliegenden Verordnung auszunehmen. Nach Artikel 2 der Richtlinie 2014/65/EU sind jedoch auch Unternehmen, die für die Zwecke der vorliegenden Verordnung als Finanzunternehmen gelten, wie Zentralverwahrer, Organismen für gemeinsame Anlagen oder Versicherungs- und Rückversicherungsunternehmen, vom Anwendungsbereich der genannten Richtlinie ausgenommen. Die Ausnahme der in den Artikeln 2 und 3 jener Richtlinie genannten Personen und Unternehmen vom Geltungsbereich der vorliegenden Verordnung sollte nicht für diese Zentralverwahrer, Organismen für gemeinsame Anlagen oder Versicherungs- und Rückversicherungsunternehmen gelten.

(42) Nach dem sektorspezifischen Unionsrecht unterliegen einige Finanzunternehmen aufgrund ihrer Größe oder den von ihnen erbrachten Dienstleistungen weniger strengen Anforderungen oder Ausnahmen. Diese Kategorie von Finanzunternehmen umfasst auch kleine und nicht verflochtene Wertpapierfirmen, kleine Einrichtungen der betrieblichen Altersversorgung, die unter den in Artikel 5 der Richtlinie (EU) 2016/2341 festgelegten Bedingungen durch die betroffenen Mitgliedstaaten vom Anwendungsbereich jener Richtlinie ausgenommen werden können und Altersversorgungssysteme betreiben, die zusammen nicht mehr als 100 Mitglieder haben, sowie gemäß der Richtlinie 2013/36/EU ausgenommene Institute. Im Einklang mit dem Grundsatz der Verhältnismäßigkeit und zur Wahrung des Geistes des sektorspezifischen Unionsrechts ist es daher auch angezeigt, diese Finanzunternehmen durch die vorliegende Verordnung einem vereinfachten IKT-Risikomanagementrahmen zu unterwerfen. Die Verhältnismäßigkeit des IKT-Risikomanagementrahmens für diese Finanzunternehmen sollte durch die von den ESA zu entwickelnden technischen Regulierungsstandards nicht verändert werden. Darüber hinaus ist es im Einklang mit dem Grundsatz der Verhältnismäßigkeit angezeigt, durch die vorliegende Verordnung auch Zahlungsinstitute im Sinne des Artikels 32 Absatz 1 der Richtlinie (EU) 2015/2366 und E-Geld-Institute im Sinne des Artikels 9 der Richtlinie 2009/110/EG, die gemäß dem nationalen Recht, das diese Rechtsakte der Union umsetzt, ausgenommen sind, einem vereinfachten IKT-Risikomanagementrahmen zu unterwerfen, während Zahlungsinstitute und E-Geld-Institute, die gemäß der jeweiligen Umsetzung des sektorspezifischen Unionsrechts nicht ausgenommen wurden, den in der vorliegenden Verordnung festgelegten allgemeinen Rahmen einhalten sollten.

(43) Ebenso sollten Finanzunternehmen, die als Kleinstunternehmen gelten oder dem vereinfachten IKT-Risikomanagementrahmen nach dieser Verordnung unterliegen, nicht verpflichtet sein, eine Funktion zur Überwachung ihrer mit IKT-Drittdienstleistern geschlossenen Vereinbarungen über die Nutzung von IKT-Dienstleistungen einzurichten oder ein Mitglied der Geschäftsleitung zu benennen, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation zuständig ist, die Verantwortung für das Management und die Überwachung von IKT-Risiken einer Kontrollfunktion zuzuweisen und zur Vermeidung von Interessenkonflikten ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicherzustellen, den IKT-Risikomanagementrahmen mindestens einmal jährlich zu dokumentieren und zu überprüfen, den IKT-Risikomanagementrahmen regelmäßig einer internen Revision zu unterziehen, nach größeren Veränderungen ihrer Netzwerk- und Informationssysteminfrastrukturen und -prozesse eingehende Bewertungen durchzuführen, regelmäßig Risikoanalysen von IKT-Altsystemen vorzunehmen, die Umsetzung der IKT-Reaktions- und Wiederherstellungspläne einer unabhängigen internen Revision zu unterziehen, eine Krisenmanagementfunktion festzulegen, die Tests der Geschäftsfortführungspläne und der Reaktions- und Wiederherstellungspläne zur Erfassung von Szenarien für die Umstellung von primärer IKT-Infrastruktur auf redundante Systeme auszuweiten, den zuständigen Behörden auf deren Anfrage eine

([18]) 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).

Schätzung der von schwerwiegenden IKT-bezogenen Vorfällen verursachten aggregierten jährlichen Kosten und Verluste vorzulegen, redundante IKT-Kapazitäten zu unterhalten, den zuständigen nationalen Behörden die nach nachträglichen Prüfungen IKT-bezogener Vorfälle vorgenommenen Änderungen zu melden, die einschlägigen technologischen Entwicklungen fortlaufend zu überwachen, als integralen Bestandteil des in dieser Verordnung vorgesehenen IKT-Risikomanagementrahmens ein umfassendes Programm für Tests der digitalen operationalen Resilienz einzurichten oder eine Strategie für das IKT-Drittparteienrisiko zu verabschieden und regelmäßig zu überprüfen. Darüber hinaus sollten Kleinstunternehmen nur verpflichtet sein, auf der Grundlage ihres Risikoprofils zu bewerten, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen. Kleinstunternehmen sollten in den Genuss einer flexibleren Regelung für Programme für Tests der digitalen operationalen Resilienz kommen. Bei der Erwägung der Art und Häufigkeit der durchzuführenden Tests sollten sie ein angemessenes Gleichgewicht zwischen dem Ziel der Aufrechterhaltung einer hohen digitalen operationalen Resilienz, den verfügbaren Ressourcen und ihrem Gesamtrisikoprofil finden. Kleinstunternehmen und Finanzunternehmen, die dem vereinfachten IKT-Risikomanagementrahmen nach dieser Verordnung unterliegen, sollten von der Verpflichtung ausgenommen werden, erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests (TLPT — Threat Led Penetration Testing) durchzuführen, da nur Finanzunternehmen, die die Kriterien in dieser Verordnung erfüllen, verpflichtet sein sollten, diese Tests durchzuführen. Angesichts ihrer begrenzten Kapazitäten sollten Kleinstunternehmen mit dem IKT-Drittdienstleister vereinbaren können, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens an einen vom IKT-Drittdienstleister zu beauftragenden unabhängigen Dritten zu delegieren, sofern das Finanzunternehmen jederzeit alle relevanten Informationen und Zusicherungen über die Leistung des IKT-Drittdienstleisters von dem jeweiligen unabhängigen Dritten anfordern kann.

(44) Da nur die Finanzunternehmen, die für die Zwecke der erweiterten Tests der digitalen Resilienz bestimmt wurden, zu bedrohungsorientierten Penetrationstests verpflichtet werden sollten, sollten die Verwaltungsverfahren und finanziellen Kosten, die mit der Durchführung dieser Tests verbunden sind, von einem kleinen Prozentsatz der Finanzunternehmen getragen werden.

(45) Um die vollständige Abstimmung und allgemeine Kohärenz zwischen den Geschäftsstrategien der Finanzunternehmen einerseits und der Durchführung des IKT-Risikomanagements andererseits zu gewährleisten, sollten die Leitungsorgane der Finanzunternehmen verpflichtet sein, beim Management und bei der Anpassung des IKT-Risikomanagementrahmens und der Gesamtstrategie für die digitale operationale Resilienz eine zentrale und aktive Rolle zu bewahren. Der von den Leitungsorganen heranzuziehende Ansatz sollte sich nicht nur auf die Mittel zur Gewährleistung der Resilienz der IKT-Systeme konzentrieren, sondern auch Menschen und Prozesse durch eine Reihe von Leit- und Richtlinien einbeziehen, die auf jeder Unternehmensebene und bei allen Mitarbeitern ein starkes Bewusstsein für Cyberrisiken und die Verpflichtung zur Einhaltung einer strengen Cyberhygiene auf allen Ebenen hervorrufen. Die letztliche Verantwortung des Leitungsorgans für das Management des IKT-Risikos eines Finanzunternehmens sollte in einem übergeordneten Prinzip dieses umfassenden Ansatzes bestehen, das sich weiter im kontinuierlichen Engagement des Leitungsorgans bei der Kontrolle der Überwachung des IKT-Risikomanagements niederschlägt.

(46) Darüber hinaus geht der Grundsatz der uneingeschränkten und letztlichen Verantwortung des Leitungsorgans für das Management der IKT-Risiken des Finanzunternehmens mit der Notwendigkeit einher, einen bestimmten Umfang von IKT-Investitionen und ein Gesamtbudget sicherzustellen, die das Finanzunternehmen in die Lage versetzen, ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(47) Aufbauend auf einschlägigen internationalen, nationalen und branchenspezifischen bewährten Verfahren, Leitlinien, Empfehlungen und Konzepten für das Management von Cyberrisiken werden mit dieser Verordnung eine Reihe von Prinzipien gefördert, die die allgemeine Struktur des IKT-Risikomanagements erleichtern. Solange die wichtigsten von Finanzunternehmen eingerichteten Kapazitäten die verschiedenen in dieser Verordnung vorgesehenen Aufgaben im IKT-Risikomanagement (Ermittlung, Schutz und Prävention, Erkennung, Reaktion und Wiederherstellung, Lernen sowie Weiterentwicklung und Kommunikation) angehen, sollte es den Finanzunternehmen folglich freistehen, IKT-Risikomanagementmodelle zu verwenden, die anders gegliedert oder kategorisiert sind.

(48) Um mit einer sich rasch ändernden Bedrohungslage Schritt zu halten, sollten Finanzunternehmen auf dem neuesten Stand befindliche IKT-Systeme unterhalten, die zuverlässig sind und nicht nur die Verarbeitung der für die Erbringung ihrer Dienste erforderlichen Daten, sondern auch ausreichende technologische Resilienz gewährleisten können, damit Finanzunternehmen in angemessener Weise auf zusätzliche Verarbeitungserfordernisse aufgrund angespannter Marktbedingungen oder anderer ungünstiger Umstände reagieren können.

(49) Effiziente Pläne zur Fortführung der Geschäftstätigkeit und für die Wiederherstellung sind erforderlich, damit Finanzunternehmen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, prompt und zügig entgegenwirken können, indem Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Maßnahmen für die Wiederherstellung im Einklang mit ihren Richtlinien für Datensicherung Vorrang erhalten. Eine solche Wiederaufnahme sollte jedoch die Integrität und Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten in keiner Weise gefährden.

(50) Mit dieser Verordnung wird Finanzunternehmen zwar ermöglicht, ihre Vorgaben für die Wiederherstellungszeit (recovery time objective) und die Wiederherstellungspunkte (recovery point objective) flexibel und daher so festzulegen, dass Art und Kritikalität der jeweiligen Funktion sowie etwaige spezifische geschäftliche Erfordernisse in vollem Umfang berücksichtigt werden, allerdings sollte bei der Festlegung dieser Vorgaben auch die Durchführung einer Bewertung der potenziellen Gesamtauswirkungen auf die Markteffizienz vorgeschrieben sein.

(51) Die Urheber von Cyberangriffen neigen dazu, finanzielle Gewinne direkt an der Quelle zu erzielen, sodass Finanzunternehmen weitreichenden Folgen ausgesetzt sind. Um zu verhindern, dass IKT-Systeme ihre Integrität einbüßen oder nicht verfügbar werden, und somit zu vermeiden, dass vertrauliche Daten eingesehen oder physische IKT-Infrastrukturen beschädigt werden, sollte die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen erheblich verbessert und gestrafft werden. Die Meldung IKT-bezogener Vorfälle sollte für alle Finanzunternehmen harmonisiert werden, indem sie verpflichtet werden, ihren jeweils zuständigen Behörden direkt Bericht zu erstatten. Unterliegt ein Finanzunternehmen der Aufsicht von mehr als einer zuständigen nationalen Behörde, so sollten die Mitgliedstaaten eine einzige zuständige Behörde als Adressat einer solchen Meldung benennen. Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 des Rates ([19]) als bedeutend eingestuft werden, sollten die Meldungen den zuständigen nationalen Behörden übermitteln, die sie anschließend an die Europäische Zentralbank (EZB) weiterleiten sollten.

(52) Die direkte Meldung sollte Finanzaufsichtsbehörden den direkten Zugang zu Informationen über schwerwiegende IKT-bezogene Vorfälle ermöglichen. Finanzaufsichtsbehörden sollten Einzelheiten über schwerwiegende IKT-bezogene Vorfälle wiederum an Nicht-Finanzbehörden (z. B gemäß der Richtlinie (EU) 2022/2555 benannte zuständige Behörden und zentrale Anlaufstellen, nationale Datenschutzbehörden und Strafverfolgungsbehörden bei schwerwiegenden IKT-bezogenen Vorfällen strafrechtlicher Art) weiterleiten, um diese Behörden für diese Vorfälle zu sensibilisieren und bei CSIRT gegebenenfalls die unverzügliche Unterstützung von Finanzunternehmen zu erleichtern. Darüber hinaus sollten die Mitgliedstaaten festlegen können, dass Finanzunternehmen selbst derartige Informationen an Behörden außerhalb des Finanzdienstleistungsbereichs weitergeben sollten. Diese Informationsflüsse sollten es Finanzunternehmen ermöglichen, rasch von allen einschlägigen technischen Informationen, der Beratung über Abhilfemaßnahmen und den anschließenden Folgemaßnahmen dieser Behörden zu profitieren. Die Informationen über schwerwiegende IKT-bezogene Vorfälle sollten wechselseitig gelenkt werden: Die Finanzaufsichtsbehörden sollten dem Finanzunternehmen alle erforderlichen Rückmeldungen oder Orientierungshilfen geben, während die ESA anonymisierte Daten über Cyberbedrohungen und Schwachstellen im Zusammenhang mit einem Vorfall austauschen sollten, um eine umfassende kollektive Verteidigung zu unterstützen.

(53) Zwar sollten alle Finanzunternehmen verpflichtet sein, Sicherheitsvorfälle zu melden, es ist jedoch davon auszugehen, dass diese Verpflichtung sie nicht alle in gleicher Weise betrifft. Die einschlägigen Wesentlichkeitsschwellen sowie die Fristen für die Meldung sollten im Rahmen delegierter Rechtsakte auf der Grundlage der von den ESA zu entwickelnden technischen Regulierungsstandards gebührend angepasst werden, um nur schwerwiegende IKT-bezogene Vorfälle abzudecken. Darüber hinaus sollten die Besonderheiten von Finanzunternehmen bei der Festlegung der Fristen für die Meldepflichten berücksichtigt werden.

(54) Diese Verordnung sollte Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute verpflichten, alle zuvor gemäß der Richtlinie (EU) 2015/2366 gemeldeten zahlungsbezogenen Betriebs- oder Sicherheitsvorfälle zu melden, unabhängig von der Art des IKT-Vorfalls.

([19]) Verordnung (EU) Nr. 1024/2013 des Rates vom 15. Oktober 2013 zur Übertragung besonderer Aufgaben im Zusammenhang mit der Aufsicht über Kreditinstitute auf die Europäische Zentralbank (ABl. L 287 vom 29.10.2013, S. 63).

(55) Die ESA sollten beauftragt werden, die Durchführbarkeit und die Bedingungen für eine mögliche Zentralisierung von Meldungen über IKT-bezogene Vorfälle auf Unionsebene zu bewerten. Eine solche Zentralisierung könnte in einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle bestehen, die die entsprechenden Meldungen entweder direkt entgegennimmt und die zuständigen nationalen Behörden automatisch benachrichtigt oder lediglich die von den zuständigen nationalen Behörden übermittelten einschlägigen Meldungen zentralisiert und somit eine Koordinierungsfunktion wahrnimmt. Die ESA sollten beauftragt werden, in Absprache mit der EZB und der ENISA einen gemeinsamen Bericht über die Machbarkeit der Einrichtung einer einheitlichen EU-Plattform auszuarbeiten.

(56) Um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen und im Einklang sowohl mit den einschlägigen internationalen Standards (z. B. die „G7 Fundamental Elements for Threat-Led Penetration Testing“ (Grundzüge bedrohungsorientierter Penetrationstests der G7-Staaten)) als auch den in der Union angewandten Rahmen (z. B. TIBER-EU), sollten Finanzunternehmen ihre IKT-Systeme und ihre Mitarbeiter mit IKT-bezogenen Verantwortungen regelmäßig auf die Effizienz ihrer Fähigkeiten für Prävention, Erkennung, Reaktion und Wiederherstellung hin testen, um potenzielle IKT-Schwachstellen aufzudecken und zu beseitigen. Um den Unterschieden Rechnung zu tragen, die zwischen und in den verschiedenen Finanzteilsektoren bei der Abwehrbereitschaft von Finanzunternehmen im Bereich der Cybersicherheit bestehen, sollten die Tests eine breite Palette von Instrumenten und Maßnahmen umfassen, die von der Bewertung grundlegender Anforderungen (z. B. Bewertungen und Überprüfungen der Schwachstellen, Analysen von Open-Source-Software, Bewertungen der Netzwerksicherheit, Lückenanalysen, Analysen der physischen Sicherheit, Fragebögen und Scansoftwarelösungen, Quellcodeprüfungen, soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests oder End-to-End-Tests) bis hin zu erweiterten Tests anhand von TLPT reichen. Diese erweiterten Tests sollten nur für Finanzunternehmen vorgeschrieben werden, die aus IKT-Perspektive ausgereift genug sind, um sie angemessen durchführen zu können. Folglich sollten die in dieser Verordnung vorgeschriebene Tests der digitalen operationalen Resilienz für die Finanzunternehmen, die die Kriterien dieser Verordnung erfüllen (zum Beispiel große systemrelevante Kreditinstitute mit ausgereifter IKT, Börsen, Zentralverwahrer und zentrale Gegenparteien), ausgedehnter sein als für andere Finanzunternehmen. Gleichzeitig sollten die Tests der digitalen operationalen Resilienz anhand von TLPT für Finanzunternehmen, die in zentralen Finanzdienstleistungsteilsektoren tätig sind und eine systemrelevante Rolle spielen (zum Beispiel Zahlungen, Banken sowie Clearing und Abrechnung), mehr Relevanz und für andere Teilsektoren (zum Beispiel Vermögensverwalter, Ratingagenturen usw.) weniger Relevanz besitzen.

(57) Grenzübergreifend tätige Finanzunternehmen, die die Niederlassungs- oder Dienstleistungsfreiheit in der Union ausüben, sollten in ihrem Herkunftsmitgliedstaat eine einheitliche Reihe von Anforderungen für erweiterte Tests (z. B. TLPT) erfüllen, die sich auf die IKT-Infrastrukturen in allen Rechtsordnungen erstrecken sollten, in denen die grenzüberschreitende Finanzgruppe innerhalb der Union tätig ist, sodass diesen grenzüberschreitend tätigen Finanzgruppen nur in einer Rechtsordnung entsprechende IKT-bezogene Testkosten entstehen.

(58) Um das Fachwissen zu nutzen, das bestimmte zuständige Behörden bereits erworben haben, insbesondere im Zusammenhang mit der Umsetzung von TIBER-EU, sollte es den Mitgliedstaaten durch diese Verordnung ermöglicht werden, auf nationaler Ebene eine einzige staatliche Behörde zu benennen, die im Finanzsektor für alle TLPT-bezogenen Fragen zuständig ist, oder — falls keine solche Behörde benannt wurde — die entsprechenden zuständigen Behörden zu benennen, die die Wahrnehmung von TLPT-bezogenen Aufgaben einer anderen zuständigen nationalen Finanzbehörde übertragen.

(59) Da Finanzunternehmen nach dieser Verordnung nicht verpflichtet sind, mit einem einzigen bedrohungsorientierten Penetrationstest alle kritischen oder wichtigen Funktionen abzudecken, sollte es den Finanzunternehmen freistehen, jeweils festzulegen, welche und wie viele kritische oder wichtige Funktionen im Rahmen dieser Tests geprüft werden sollten.

(60) Gebündelte Tests im Sinne dieser Verordnung — bei denen verschiedene Finanzunternehmen an einem TLPT teilnehmen und ein IKT-Drittdienstleister zu diesem Zweck direkt vertragliche Vereinbarungen mit einem externen Tester eingehen kann — sollten nur dann zulässig sein, wenn gerechtfertigt von nachteiligen Auswirkungen auf die Qualität oder Sicherheit derjenigen Dienstleistungen ausgegangen werden kann, die der IKT-Drittdienstleister für Kunden erbringt, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit von mit diesen Dienstleistungen in Verbindung stehenden Daten. Gebündelte Tests sollten auch Schutzvorkehrungen unterliegen (Leitung durch ein benanntes Finanzunternehmen, Abgleich der Anzahl der teilnehmenden Finanzunternehmen), damit ein strenges Testverfahren für diejenigen beteiligten Finanzunternehmen gewährleistet ist, die den Zielen des TLPT gemäß dieser Verordnung gerecht werden.

(61) Um die auf Unternehmensebene verfügbaren internen Ressourcen zu nutzen, sollte der Einsatz interner Tester zur Durchführung von TLPT gemäß dieser Verordnung gestattet sein, sofern eine aufsichtliche Genehmigung vorliegt, keine Interessenkonflikte bestehen und ein regelmäßiger Wechsel (jeweils nach drei Tests) im Einsatz von internen und externen Testern stattfindet, wobei es sich zudem bei dem Anbieter der Bedrohungsanalyse im Rahmen der TLPT stets um ein Unternehmen außerhalb des betreffenden Finanzunternehmens handeln muss. Die Durchführung von TLPT sollten weiterhin uneingeschränkt in der Verantwortung der Finanzunternehmen liegen. Die von den Behörden ausgestellten Bescheinigungen sollten ausschließlich dem Zweck der gegenseitigen Anerkennung dienen und sollten weder Folgemaßnahmen ausschließen, die erforderlich sind, um IKT-Risiken, denen das Finanzunternehmen ausgesetzt ist, anzugehen, noch sollten sie als aufsichtliche Billigung der IKT-Risikomanagement- und -minderungsfähigkeiten eines Finanzunternehmens betrachtet werden.

(62) Um eine solide Überwachung des IKT-Drittparteienrisikos im Finanzsektor zu gewährleisten, sind eine Reihe grundsatzbasierter Regeln festzulegen, um Finanzunternehmen bei der Überwachung der Risiken anzuleiten, die im Zusammenhang mit an IKT-Drittdienstleister ausgelagerten Funktionen — insbesondere mit IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen — sowie ganz allgemein im Zusammenhang mit jeglichen Abhängigkeiten von IKT-Drittdienstleistern entstehen.

(63) Um der Komplexität der verschiedenen IKT-Risikoquellen und dabei zugleich der Vielzahl und Vielfalt der Anbieter technologischer Lösungen, die eine reibungslose Erbringung von Finanzdienstleistungen ermöglichen, gerecht zu werden, sollte diese Verordnung für ein breites Spektrum von IKT-Drittdienstleistern gelten, darunter Anbieter von Cloud-Computing-Diensten, Software, Datenanalysediensten und Anbieter von Rechenzentrumsdienstleistungen. Da Finanzunternehmen alle Arten von Risiken — auch im Zusammenhang mit innerhalb einer Finanzgruppe beschafften IKT-Dienstleistungen — wirksam und kohärent ermitteln und managen sollten, sollte zudem klar herausgestellt werden, dass Unternehmen, die Teil einer Finanzgruppe sind und IKT-Dienstleistungen vorwiegend für ihr Mutterunternehmen oder für Tochterunternehmen oder Zweigniederlassungen ihres Mutterunternehmens erbringen, sowie Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen erbringen, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten sollten. Angesichts der zunehmenden Abhängigkeit des sich entwickelnden Marktes für Zahlungsdienste von komplexen technischen Lösungen sowie angesichts neu entstehender Arten von Zahlungsdiensten und zahlungsbezogenen Lösungen sollten diejenigen Teilnehmer des Ökosystems für Zahlungsdienste, die Zahlungsabwicklungstätigkeiten durchführen oder Zahlungsinfrastrukturen betreiben, ebenfalls als IKT-Drittdienstleister im Sinne dieser Verordnung gelten, mit Ausnahme von Zentralbanken, die Zahlungs- oder Wertpapierliefer- und -abrechnungssysteme betreiben, und von staatlichen Behörden, die IKT-bezogene Dienste im Zusammenhang mit Funktionen des Staates bereitstellen.

(64) Ein Finanzunternehmen sollte jederzeit die volle Verantwortung für die Einhaltung seiner Verpflichtungen aus dieser Verordnung tragen. Die Finanzunternehmen sollten bei der Überwachung der Risiken, die auf Ebene der IKT-Drittdienstleister entstehen, einen verhältnismäßigen Ansatz verfolgen, indem Art, Umfang, Komplexität und Bedeutung ihrer IKT-bezogener Abhängigkeiten und die Kritikalität oder Bedeutung der Dienste, Prozesse oder Funktionen, die den vertraglichen Vereinbarungen unterliegen, letztlich je nach Sachlage anhand einer sorgfältigen Bewertung jeglicher potenzieller Auswirkungen auf die Kontinuität und Qualität von Finanzdienstleistungen auf Einzel- und Gruppenebene gebührend berücksichtigt werden.

(65) Die Durchführung einer solchen Überwachung sollte nach einem strategischen Ansatz für das IKT-Drittparteienrisiko erfolgen, der durch die Annahme einer eigenen Strategie für das von IKT-Drittdienstleistern ausgehende Risiko durch das Leitungsorgan des Finanzunternehmens formalisiert wird, und zwar auf der Grundlage einer kontinuierlichen Überprüfung aller Abhängigkeiten von IKT-Drittdienstleistern. Um die Aufsichtsbehörden für Abhängigkeiten von IKT-Drittdienstleistern zu sensibilisieren und die Arbeiten im Zusammenhang mit dem durch diese Verordnung geschaffenen Überwachungsrahmen weiter zu unterstützen, sollten sämtliche Finanzunternehmen verpflichtet werden, ein Informationsregister mit allen vertraglichen Vereinbarungen betreffend die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden, zu führen. Die Finanzaufsichtsbehörden sollten in der Lage sein, das vollständige Register oder bestimmte Abschnitte des Registers anzufordern und somit wesentliche Informationen zu erhalten, die ein umfassenderes Verständnis der IKT-bezogenen Abhängigkeiten von Finanzunternehmen ermöglichen.

(66) Dem förmlichen Abschluss vertraglicher Vereinbarungen sollte eine gründliche Analyse vor Vertragsabschluss zugrunde liegen und diesem vorausgehen, insbesondere indem der Fokus auf Aspekte wie die Kritikalität oder Bedeutung der durch den geplanten IKT-Vertrag unterstützten Dienste, die erforderlichen aufsichtlichen Genehmigungen oder sonstigen Bedingungen, das damit verbundene mögliche Konzentrationsrisiko sowie die Anwendung der Sorgfaltspflicht bei der Auswahl und Bewertung von IKT-Drittdienstleistern gelegt wird, und indem potenzielle Interessenkonflikte bewertet werden. Betreffen vertragliche Vereinbarungen kritische oder wichtige Funktionen, so sollten Finanzunternehmen darauf achten, dass IKT-Drittdienstleister die aktuellsten und höchsten Standards für die Informationssicherheit anwenden. Die Kündigung vertraglicher Vereinbarungen könnte zumindest

durch eine Reihe von Umständen ausgelöst werden, die Unzulänglichkeiten auf Ebene des IKT-Drittdienstleister erkennen lassen, insbesondere erhebliche Verstöße gegen Rechtsvorschriften oder Vertragsbestimmungen, Umstände, die auf eine potenzielle Änderung der Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen hindeuten, Hinweise auf Schwachstellen beim allgemeinen IKT-Risikomanagement des IKT-Drittdienstleisters oder Umstände, die darauf hinweisen, dass die jeweils zuständige Behörde nicht zu einer wirksamen Beaufsichtigung des Finanzunternehmens in der Lage sind.

(67) Um die systemischen Auswirkungen des Konzentrationsrisikos von IKT-Drittdienstleistern zu anzugehen, wird mit dieser Verordnung eine ausgewogene Lösung angestrebt, indem bei solchen Konzentrationsrisiken ein flexibler und schrittweiser Ansatz verfolgt wird, da jegliche vorgeschriebene starre Obergrenzen oder strenge Beschränkungen die Geschäftstätigkeit behindern und die Vertragsfreiheit beeinträchtigen können. Finanzunternehmen sollten ihre geplanten vertraglichen Vereinbarungen gründlich prüfen, um die Wahrscheinlichkeit des Auftretens eines solchen Risikos zu ermitteln, unter anderem durch fundierte Analysen von Unterauftragsvereinbarungen, insbesondere wenn diese mit IKT-Drittdienstleistern geschlossen werden, die in einem Drittland niedergelassen sind. Um ein ausgewogenes Verhältnis zwischen dem Sachzwang, zum einen die Vertragsfreiheit zu wahren und zum anderen die Finanzstabilität zu gewährleisten, wird es zum gegenwärtigen Zeitpunkt nicht als zweckmäßig erachtet, strenge Obergrenzen und Beschränkungen für die Exposition gegenüber IKT-Drittdienstleistern festzulegen. Was kritische IKT-Drittdienstleister anbelangt, so sollte eine nach dieser Verordnung ernannte federführende Überwachungsbehörde bei der Wahrnehmung ihrer Aufsichtsaufgaben im Kontext des Überwachungsrahmens besonders darauf achten, das Ausmaß der Interdependenzen voll zu erfassen, spezifische Fälle zu ermitteln, in deren Rahmen eine hohe Konzentration kritischer IKT-Drittdienstleister in der Union die Stabilität und Integrität des Finanzsystems der Union belasten dürfte, sowie einen Dialog mit kritischen IKT-Drittdienstleistern zu führen, bei denen dieses spezifische Risiko ermittelt wird.

(68) Um die Fähigkeit eines IKT-Drittdienstleisters, sichere Dienstleistungen für ein Finanzunternehmen ohne nachteilige Auswirkungen auf dessen digitale operationale Resilienz zu erbringen, regelmäßig zu bewerten und zu überwachen, sollten einige wesentliche Vertragsbestandteile mit IKT-Drittdienstleistern harmonisiert werden. Diese Harmonisierung sollte Mindestbereiche abdecken, die — unter dem Gesichtspunkt, dass ein Finanzunternehmen seine digitale Resilienz sicherstellen muss, da es in hohem Maße von der Stabilität, der Funktionalität, der Verfügbarkeit und der Sicherheit der beanspruchten IKT-Dienstleistungen abhängig ist — für eine umfassende Überwachung der von einem IKT-Drittdienstleister möglicherweise ausgehenden Risiken durch das Finanzunternehmen von entscheidender Bedeutung sind.

(69) Bei der Neuaushandlung vertraglicher Vereinbarungen zwecks Angleichung an die Anforderungen dieser Verordnung sollten Finanzunternehmen und IKT-Drittdienstleister sicherstellen, dass die in dieser Verordnung vorgesehenen wesentlichen Vertragsbestimmungen berücksichtigt werden.

(70) Die Begriffsbestimmung der „kritischen oder wichtigen Funktion“ im Sinne dieser Verordnung schließt auch die Begriffsbestimmung der „kritischen Funktionen“ im Sinne von Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates ([20]) ein. Dementsprechend sind die gemäß der Richtlinie 2014/59/EU als kritisch eingestuften Funktionen in der Begriffsbestimmung der kritischen Funktionen im Sinne dieser Verordnung ebenfalls erfasst.

(71) Ungeachtet der Kritikalität oder Bedeutung der von dem IKT-Drittdienstleister unterstützten Funktion sollte in den vertraglichen Vereinbarungen insbesondere eine Spezifikation der vollständigen Beschreibungen von Funktionen und Dienstleistungen sowie von Orten, an denen solche Funktionen bereitgestellt werden und Daten verarbeitet werden sollen, vorgesehen sein; ferner sollten Beschreibungen der Dienstleistungsgüte enthalten sein. Andere wesentliche Elemente um einem Finanzunternehmen die Überwachung des IKT-Drittparteienrisikos zu ermöglichen, sind die Folgenden: vertragliche Bestimmungen dazu, wie Zugänglichkeit, Verfügbarkeit, Integrität, Sicherheit und Schutz personenbezogener Daten durch den IKT-Drittdienstleister gewährleistet werden; Bestimmungen über die einschlägigen Garantien für den Zugang zu sowie die Wiederherstellung und Rückgabe von Daten im Falle einer Insolvenz, Abwicklung oder Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters; Bestimmungen, die den IKT-Drittdienstleister dazu verpflichten, im Falle von IKT-Vorfällen im Zusammenhang mit den erbrachten Dienstleistungen ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu

([20]) Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

leisten; Bestimmungen über die Verpflichtung des IKT-Drittdienstleisters, uneingeschränkt mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, sowie Bestimmungen über Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und Abwicklungsbehörden.

(72) In Ergänzung zu derartigen vertraglichen Bestimmungen sowie um sicherzustellen, dass Finanzunternehmen die volle Kontrolle über alle von Dritten ausgehenden Entwicklungen behalten, die ihre IKT-Sicherheit beeinträchtigen könnten, sollten die Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen zudem Folgendes vorschreiben: die Spezifikation der vollständigen Beschreibung der Dienstleistungsgüte einschließlich präziser quantitativer und qualitativer Leistungsziele, damit unverzüglich angemessene Korrekturmaßnahmen ergriffen werden können, wenn die vereinbarte Dienstleistungsgüte nicht erreicht werden; die einschlägigen Kündigungsfristen und Meldepflichten des IKT-Drittdienstleisters im Falle von Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters auswirken könnten, die entsprechenden IKT-Dienstleistungen wirksam zur Verfügung stellen; die Anforderung an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu erproben und über Maßnahmen, Instrumente und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die eine sichere Erbringung von Dienstleistungen ermöglichen, sowie sich an dem TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken.

(73) Verträge über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sollten zudem Bestimmungen enthalten, die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten sowie das Recht auf Anfertigung von Kopien regeln, die als wesentliche Instrumente für die laufende Überwachung der Leistung des IKT-Drittdienstleisters durch die Finanzunternehmen dienen, gepaart mit der uneingeschränkten Zusammenarbeit des Drittdienstleisters während der Inspektionen. In gleicher Weise sollte die für das Finanzunternehmen zuständige Behörde auf der Grundlage von Mitteilungen über das Recht verfügen, den IKT-Drittdienstleister vorbehaltlich des Schutzes vertraulicher Informationen zu inspizieren und zu prüfen.

(74) Diese vertraglichen Vereinbarungen sollten ferner spezielle Ausstiegsstrategien vorsehen, die insbesondere verbindliche Übergangszeiträume ermöglichen, in denen die IKT-Drittdienstleister weiterhin die einschlägigen Dienste bereitstellen sollten, um das Risiko von Störungen auf Ebene des Finanzunternehmens zu verringern oder es Letzterem zu ermöglichen, effektiv zu anderen IKT-Drittdienstleistern zu wechseln oder alternativ zu internen Lösungen zu wechseln, die der Komplexität der bereitgestellten IKT-Dienstleistungen entsprechen. Darüber hinaus sollten Finanzunternehmen, die in den Geltungsbereich der Richtlinie 2014/59/EU fallen, sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen solide und im Falle der Abwicklung dieser Finanzunternehmen uneingeschränkt durchsetzbar sind. Daher sollten diese Finanzunternehmen im Einklang mit den Erwartungen der Abwicklungsbehörden sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen abwicklungssicher sind. Solange diese Finanzunternehmen ihren Zahlungsverpflichtungen weiterhin nachkommen, sollten sie neben anderen Anforderungen sicherstellen, dass die einschlägigen Verträge über IKT-Dienstleistungen Klauseln darüber enthalten, dass sie nicht aufgrund einer Umstrukturierung oder Abwicklung gekündigt, ausgesetzt oder geändert werden können.

(75) Darüber hinaus kann die freiwillige Verwendung von Standardvertragsklauseln, die von staatlichen Behörden oder von Organen der Union entwickelt wurden, insbesondere die Verwendung von der Kommission für Cloud-Computing Dienste entwickelten Vertragsklauseln den Finanzunternehmen und IKT-Drittdienstleistern eine zusätzliche Rückversicherung bieten, indem sie die Rechtssicherheit in Bezug auf die Nutzung von Cloud-Computing-Diensten im Finanzsektor in voller Übereinstimmung mit den Anforderungen und Erwartungen des Finanzdienstleistungsrechts der Union erhöht. Die Erarbeitung von Standardvertragsklauseln baut auf Maßnahmen auf, die bereits im FinTech-Aktionsplan von 2018 vorgesehen waren, in dem die Absicht der Kommission angekündigt wurde, die Entwicklung von Standardvertragsklauseln für die Auslagerung von Cloud-Computing-Dienstleistungen durch Finanzunternehmen zu fördern und zu erleichtern, wobei auf den sektorübergreifenden Anstrengungen der Cloud-Interessenträger aufgebaut wird, die die Kommission unter Beteiligung des Finanzsektors unterstützt hat.

(76) Um die Konvergenz und Effizienz von Aufsichtskonzepten in Bezug auf das IKT-Drittparteienrisiko im Finanzsektor zu fördern und um die digitale operationale Resilienz von Finanzunternehmen zu stärken, die bei den IKT-Dienstleistungen, die die Erbringung von Finanzdienstleistungen unterstützen, auf kritische IKT-Drittdienstleister angewiesen sind, und damit zugleich dazu beizutragen, die Stabilität des Finanzsystems der Union und die Integrität des Binnenmarkts für Finanzdienstleistungen zu bewahren, sollten kritische IKT-Drittdienstleister einem Überwachungsrahmen der Union unterliegen. Auch wenn die Einrichtung des Überwachungsrahmens aufgrund des Mehrwerts von Maßnahmen auf Unionsebene und der inhärenten Rolle und der Besonderheiten der Nutzung von

IKT-Dienstleistungen bei der Erbringung von Finanzdienstleistungen gerechtfertigt ist, sollte zugleich daran erinnert werden, dass diese Lösung nur im Kontext dieser Verordnung, die speziell der digitalen operationalen Resilienz im Finanzsektor vorbehalten ist, angemessen erscheint. Ein solcher Überwachungsrahmen sollte hingegen nicht als ein neues Modell für die Beaufsichtigung auf Ebene der Union in den Bereichen Finanzdienstleistungen und -tätigkeiten betrachtet werden.

(77) Der Überwachungsrahmen sollte nur für kritische IKT-Drittdienstleister gelten. Daher sollte es einen Einstufungsmechanismus geben, um dem Ausmaß und der Art der Abhängigkeit des Finanzsektors von solchen IKT-Drittdienstleistern Rechnung zu tragen. Dieser Mechanismus sollte eine Reihe quantitativer und qualitativer Kriterien umfassen, mit denen die Kritikalitätsparameter als Grundlage für die Einbeziehung in den Überwachungsrahmen festgelegt würden. Um eine akkurate Bewertung zu gewährleisten, sollten diese Kriterien unabhängig von der Unternehmensstruktur des IKT-Drittdienstleisters im Falle eines IKT-Drittdienstleisters, der Teil einer größeren Gruppe ist, die gesamte Gruppenstruktur des IKT-Drittdienstleisters berücksichtigen. Einerseits sollten kritische IKT-Drittdienstleister, die aufgrund der Anwendung der oben genannten Kriterien nicht automatisch eingestuft werden, die Möglichkeit haben, sich auf freiwilliger Basis für den Überwachungsrahmen zu entscheiden, andererseits sollten IKT-Drittdienstleister, die bereits Überwachungsmechanismen unterliegen, die die Erfüllung der in Artikel 127 Absatz 2 AEUV genannten Aufgaben des Europäischen Systems der Zentralbanken unterstützen, ausgenommen werden.

(78) Ebenso sollten Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen, zugleich aber der von dieser Verordnung erfassten Kategorie von IKT-Drittdienstleistern angehören, ebenfalls von dem Überwachungsrahmen ausgenommen werden, da sie bereits den Aufsichtsmechanismen unterliegen, die durch das einschlägige Finanzdienstleistungsrecht der Union geschaffen wurden. Wenn zweckmäßig sollten die zuständigen Behörden im Rahmen ihrer Aufsichtstätigkeiten das IKT-Risiko berücksichtigen, das von den IKT-Dienstleistungen bereitstellenden Finanzunternehmen für andere Finanzunternehmen ausgeht. In gleicher Weise sollte aufgrund der auf Gruppenebene bestehenden Risikoüberwachungsmechanismen dieselbe Ausnahme für diejenigen IKT-Drittdienstleister vorgesehen werden, die Dienstleistungen vorwiegend für die ihrer eigenen Gruppe angehörenden Unternehmen erbringen. IKT-Drittdienstleister, die lediglich in einem Mitgliedstaat IKT-Dienstleistungen für Finanzunternehmen bereitstellen, die nur in diesem Mitgliedstaat tätig sind, sollten aufgrund ihrer begrenzten Tätigkeiten und der fehlenden grenzüberschreitenden Auswirkungen ebenfalls von dem Einstufungsmechanismus ausgenommen werden.

(79) Der digitale Wandel im Bereich der Finanzdienstleistungen hat zu einem noch nie da gewesenen Maß an Nutzung und Abhängigkeit von IKT-Dienstleistungen geführt. Da es unvorstellbar geworden ist, Finanzdienstleistungen ohne die Nutzung von Cloud-Computing-Diensten, Softwarelösungen und datenbezogenen Dienstleistungen zu erbringen, ist das Finanzökosystem der Union zwangsläufig immer abhängiger von bestimmten IKT-Dienstleistungen geworden, die von IKT-Dienstleistern bereitgestellt werden. Einige dieser Dienstleister sind Innovatoren bei der Entwicklung und Anwendung IKT-gestützter Technologien und spielen daher eine wichtige Rolle bei der Erbringung von Finanzdienstleistungen oder sind nunmehr fester Bestandteil der Wertschöpfungskette für Finanzdienstleistungen geworden. Somit sind sie für die Stabilität und Integrität des Finanzsystems der Union inzwischen von entscheidender Bedeutung. Diese breite Abhängigkeit von Dienstleistungen, die von kritischen IKT-Drittdienstleistern erbracht werden, in Verbindung mit der Interdependenz der Informationssysteme verschiedener Marktteilnehmer schafft ein unmittelbares und potenziell schwerwiegendes Risiko für das Finanzdienstleistungssystem der Union und für die Kontinuität bei der Erbringung von Finanzdienstleistungen, falls kritische IKT-Drittdienstleister von Betriebsstörungen oder schwerwiegenden Cybervorfällen betroffen sein sollten. Cybervorfälle haben die Besonderheit, dass sie sich im gesamten Finanzsystem potenzieren und erheblich schneller verbreiten können als andere Arten von Risiken, die im Finanzsektor überwacht werden, und sich über Branchen und geografische Grenzen hinweg ausbreiten können. Sie haben das Potenzial, sich zu einer Systemkrise auszuweiten, bei der das Vertrauen in das Finanzsystem aufgrund der Unterbrechung von Funktionen zur Stützung der Realwirtschaft oder aufgrund erheblicher finanzieller Verluste auf ein Niveau sinkt, dem das Finanzsystem nicht standhalten kann oder das gezielte Maßnahmen zur Abfederung schwerer Schocks erfordert. Um zu verhindern, dass diese Szenarien eintreten und dabei die Stabilität und Integrität des Finanzsystems der Union gefährden, ist es von entscheidender Bedeutung, die Aufsichtspraktiken hinsichtlich des IKT-Drittparteienrisikos im Finanzsektor einander anzunähern, insbesondere durch neue Vorschriften, die die Überwachung kritischer IKT-Drittdienstleister in der Union ermöglichen.

(80) Der Überwachungsrahmen hängt weitgehend vom Ausmaß der Zusammenarbeit zwischen der federführenden Überwachungsbehörde und dem kritischen IKT-Drittdienstleister ab, der Dienste für Finanzunternehmen bereitstellt, die sich auf die Erbringung von Finanzdienstleistungen auswirken. Eine erfolgreiche Überwachung setzt unter anderem voraus, dass die federführende Überwachungsbehörde in der Lage ist, Überwachungsmissionen und Inspektionen effektiv durchzuführen, um die von kritischen IKT-Drittdienstleistern angewandten Regeln, Kontrollen und Verfahren sowie die potenziellen kumulativen Auswirkungen ihrer Tätigkeiten auf die Finanzstabilität und die Integrität des Finanzsystems zu bewerten. Gleichzeitig ist es entscheidend, dass kritische IKT-Drittdienstleister die Empfehlungen der federführenden Überwachungsbehörde befolgen und deren Bedenken ausräumen. Da ein kritischer IKT-Drittdienstleister, der Dienste bereitstellt, die sich auf die Erbringung von Finanzdienstleistungen auswirken, durch seine mangelnde Zusammenarbeit — beispielsweise indem er den Zugang zu seinen Räumlichkeiten oder die Übermittlung von Informationen verweigert — der federführenden Überwachungsbehörde letztlich ihre wichtigsten Instrumente zur Bewertung des IKT-Drittparteienrisikos nehmen würde und die Finanzstabilität und die Integrität des Finanzsystems dadurch beeinträchtigt werden könnten, ist auch eine angemessene Sanktionsregelung vorzusehen.

(81) Vor diesem Hintergrund sollte die Anforderung, dass eine federführende Überwachungsbehörde Zwangsgelder verhängen können muss, um kritische IKT-Drittdienstleister zur Einhaltung der in dieser Verordnung festgelegten Transparenz- und Zugangsverpflichtungen zu zwingen, nicht durch Schwierigkeiten gefährdet werden, die bei der Durchsetzung dieser Zwangsgelder in Bezug auf kritische IKT-Drittdienstleister mit Sitz in einem Drittland auftreten können. Um solche Sanktionen durchsetzen zu können und eine rasche Aufnahme von Verfahren zur Wahrung der Verteidigungsrechte kritischer IKT-Drittdienstleister im Zusammenhang mit dem Einstufungsmechanismus und der Herausgabe von Empfehlungen zu ermöglichen, sollten diese kritische IKT-Drittdienstleister, die Dienste für Finanzunternehmen bereitstellen, die sich auf die Erbringung von Finanzdienstleistungen auswirken, dazu verpflichtet werden, eine angemessene geschäftliche Präsenz in der Union aufrechtzuerhalten. Aufgrund der Art der Überwachung und fehlender vergleichbarer Regelungen in anderen Rechtsordnungen gibt es keine geeigneten alternativen Mechanismen, die diesem Ziel genügen, indem bei der Überwachung der Auswirkungen digitaler operationeller Risiken, die von systemrelevanten, als kritisch eingestuften IKT-Drittdienstleistern mit Sitz in einem Drittland ausgehen, effektiv mit den Finanzaufsichtsbehörden in Drittländern zusammengearbeitet wird. Um weiterhin kontinuierlich IKT-Dienstleistungen für Finanzunternehmen in der Union bereitstellen zu können, sollte ein IKT-Drittdienstleister mit Sitz in einem Drittland, der als kritisch im Sinne dieser Verordnung eingestuft worden ist, daher innerhalb von zwölf Monaten nach dieser Einstufung alle erforderlichen Vorkehrungen treffen, um seine Eingliederung in die Union mittels Gründung eines Tochterunternehmens im Sinne des Besitzstands der Union, namentlich der Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates ([21]), sicherzustellen.

(82) Die Anforderung, in der Union ein Tochterunternehmen zu gründen, sollte den kritischen IKT-Drittdienstleister nicht daran hindern, IKT-Dienstleistungen und damit verbundene technische Unterstützung von außerhalb der Union gelegenen Einrichtungen und Infrastruktur aus bereitzustellen. Diese Verordnung auferlegt keine Verpflichtung zur Lokalisierung von Daten, da sie keine Speicherung oder Verarbeitung von Daten in der Union vorschreibt.

(83) Kritische IKT-Drittdienstleister sollten in der Lage sein, IKT-Dienstleistungen von jedem beliebigen Ort der Welt aus zu erbringen, nicht unbedingt oder ausschließlich von einem in der Union gelegenen Ort aus. Die Überwachungstätigkeiten sollten zunächst an einem Ort in der Union und im Wege der Interaktion mit in der Union gelegenen Unternehmen, einschließlich der von kritischen IKT-Drittdienstleistern im Sinne dieser Verordnung gegründeten Tochterunternehmen, durchgeführt werden. Diese Maßnahmen innerhalb der Union reichen jedoch möglicherweise nicht aus, um der federführenden Überwachungsbehörde die uneingeschränkte und wirksame Wahrnehmung ihrer Aufgaben im Rahmen dieser Verordnung zu ermöglichen. Die federführende Überwachungsbehörde sollte daher ihre einschlägigen Überwachungsbefugnisse auch in Drittländern ausüben können. Durch die Ausübung dieser Befugnisse in Drittländern sollte es der federführenden Überwachungsbehörde möglich sein, die Einrichtungen zu prüfen, von denen aus die IKT-Dienstleistungen oder die technischen Unterstützungsdienste tatsächlich von dem kritischen IKT-Drittdienstleister bereitgestellt oder betrieben werden, und ein umfassendes und operatives Verständnis des IKT-Risikomanagements des kritischen IKT-Drittdienstleisters zu erhalten. Die Möglichkeit, dass die federführende Überwachungsbehörde als Agentur der Union Befugnisse außerhalb des Gebiets der Union ausübt, sollte durch Festschreibung der einschlägigen Voraussetzungen, insbesondere der Zustimmung des betreffenden kritischen IKT-Drittdienstleisters, klar geregelt werden. Ebenso sollten die einschlägigen Behörden des Drittlandes darüber unterrichtet sein, welche Tätigkeiten die federführende Überwachungsbehörde im Hoheitsgebiet des

([21]) Richtlinie 2013/34/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Jahresabschluss, den konsolidierten Abschluss und damit verbundene Berichte von Unternehmen bestimmter Rechtsformen und zur Änderung der Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinien 78/660/EWG und 83/349/EWG des Rates (ABl. L 182 vom 29.6.2013, S. 19).

betreffenden Drittlands ausübt, und keine Einwände dagegen erhoben haben. Um jedoch eine effiziente Umsetzung zu gewährleisten, müssen diese Befugnisse unbeschadet der jeweiligen Zuständigkeiten der Organe der Union bzw. der Mitgliedstaaten beim Abschluss von Vereinbarungen über die Verwaltungszusammenarbeit mit den einschlägigen Behörden des betreffenden Drittlands darin vollständig verankert werden. Diese Verordnung sollte es den ESA daher ermöglichen, mit den einschlägigen Behörden von Drittländern Vereinbarungen über die Verwaltungszusammenarbeit zu schließen, die keine anderweitigen rechtlichen Verpflichtungen gegenüber der Union und ihren Mitgliedstaaten begründen sollten.

(84) Um die Kommunikation mit der federführenden Überwachungsbehörde zu erleichtern und eine angemessene Vertretung sicherzustellen, sollten kritische IKT-Drittdienstleister, die Teil einer Gruppe sind, eine juristische Person als ihre Koordinierungsstelle benennen.

(85) Der Überwachungsrahmen sollte die Befugnis der Mitgliedstaaten unberührt lassen, eigene Aufsichts- oder Überwachungsmissionen in Bezug auf IKT-Drittdienstleister durchzuführen, die im Rahmen dieser Verordnung zwar nicht als kritisch eingestuft werden, aber auf nationaler Ebene als wichtig angesehen werden.

(86) Um die mehrschichtige institutionelle Architektur im Bereich der Finanzdienstleistungen zu nutzen, sollte der Gemeinsame Ausschuss der ESA im Einklang mit seinen Aufgaben im Bereich Cybersicherheit weiterhin die sektorübergreifende Gesamtkoordinierung für alle Fragen im Zusammenhang mit IKT-Risiken gewährleisten. Er sollte dabei durch einen neuen Unterausschuss (Überwachungsforum) unterstützt werden, der sowohl Einzelentscheidungen, die sich an kritische IKT-Drittdienstleister richten, als auch die Herausgabe gemeinsamer Empfehlungen, insbesondere in Bezug auf das Benchmarking der Überwachungsprogramme kritischer IKT-Drittdienstleister und zur Ermittlung bewährter Verfahren zur Bewältigung von Problemen im Zusammenhang mit IKT-Konzentrationsrisiken, vorbereitet.

(87) Um sicherzustellen, dass kritische IKT-Drittdienstleister auf Unionsebene angemessen und wirksam überwacht werden, könnte nach dieser Verordnung jede der drei ESA als federführende Überwachungsbehörde benannt werden. Die Entscheidung darüber, welcher der drei ESA ein kritischer IKT-Drittdienstleister konkret zugewiesen wird, sollte anhand einer Bewertung dessen getroffen werden, welche Finanzunternehmen in den Finanzbranchen, für die die betreffende ESA zuständig ist, überwiegend tätig sind. Dieser Ansatz sollte zu einer ausgewogenen Aufteilung der Aufgaben und Zuständigkeiten zwischen den drei ESA bei der Wahrnehmung ihrer Überwachungsfunktionen führen und die Humanressourcen und das technische Fachwissen, über die jede der drei ESA verfügen, bestmöglich nutzen.

(88) Federführende Überwachungsbehörden sollten mit den erforderlichen Befugnissen ausgestattet werden, Untersuchungen sowie Inspektionen vor Ort und von außerhalb bei kritischen IKT-Drittdienstleistern in deren Räumlichkeiten und an deren Standorten durchzuführen und vollständige und aktuelle Informationen zu erhalten. Diese Befugnisse sollten es der federführenden Überwachungsbehörde ermöglichen, Art, Ausmaß und Auswirkungen des IKT-Drittparteienrisikos für die Finanzunternehmen und letztlich für das Finanzsystem der Union, wahrheitsgetreu erfassen zu können. Die Übertragung der federführenden Überwachung auf die ESA ist eine Voraussetzung dafür, die systemische Dimension des IKT-Risikos im Finanzwesen zu verstehen und zu berücksichtigen. Der Einfluss kritischer IKT-Drittdienstleister auf den Finanzsektor der Union und die potenziellen Probleme, die durch das damit verbundene IKT-Konzentrationsrisiko verursacht werden, erfordern einen kollektiven Ansatz auf Unionsebene. Die gleichzeitige Durchführung mehrfacher Audits und Wahrnehmung von Zugangsrechten, die zahlreiche zuständige Behörden gesondert unter geringer oder keinerlei Abstimmung vornehmen, würden die Finanzaufsichtsbehörden daran hindern, sich einen vollständigen und umfassenden Überblick über das IKT-Drittparteienrisiko in der Union zu verschaffen und zudem gleichzeitig Redundanz, Belastungen und Komplexität für kritische IKT-Drittdienstleister mit sich bringen, wenn sie mit einer Vielzahl von Überwachungs- und Inspektionsanfragen konfrontiert sind.

(89) Aufgrund der erheblichen Auswirkungen, die mit der Einstufung als kritischer IKT-Drittdienstleister verbunden sind, sollte mit dieser Verordnung sichergestellt werden, dass die Rechte kritischer IKT-Drittdienstleister während der Umsetzung des Überwachungsrahmens gewahrt werden. Bevor sie als kritisch eingestuft werden, sollten diese Dienstleister beispielsweise berechtigt sein, der federführenden Überwachungsbehörde eine mit Gründen versehene Erklärung vorzulegen, die alle für die Beurteilung ihrer Einstufung relevanten Informationen enthält. Da die federführende Überwachungsbehörde befugt sein sollte, Empfehlungen zu IKT-Risiken und diesbezüglich geeigneten Abhilfemaßnahmen herauszugeben, was auch die Befugnis einschließt, bestimmte vertragliche Vereinbarungen, die letztlich die Stabilität des Finanzunternehmens oder des Finanzsystems beeinträchtigen, abzulehnen, sollte kritischen IKT-Drittdienstleistern ebenfalls die Möglichkeit eingeräumt werden, vor der Fertigstellung dieser Empfehlungen darzulegen, wie sich die darin aufgezeigten Lösungen voraussichtlich auf

Kunden auswirken werden, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, sowie Lösungen zur Risikominderung aufzuzeigen. Kritische IKT-Drittdienstleister, die den Empfehlungen nicht zustimmen, sollten eine begründete Erklärung über ihre Absicht, die Empfehlung nicht zu billigen, abgeben. Wird eine solche begründete Erklärung nicht abgegeben oder als unzureichend erachtet, sollte die federführende Überwachungsbehörde eine Mitteilung veröffentlichen, in der die strittige Angelegenheit kurz dargelegt wird.

(90) Die zuständigen Behörden sollten die Aufgabe, die inhaltliche Einhaltung der von der federführenden Überwachungsbehörde herausgegebenen Empfehlungen zu überprüfen, im Rahmen ihrer Tätigkeiten zur Beaufsichtigung von Finanzunternehmen gebührend wahrnehmen. Die zuständigen Behörden sollten Finanzunternehmen dazu verpflichten können, zusätzliche Maßnahmen zu ergreifen, um den in den Empfehlungen der federführenden Überwachungsbehörde ermittelten Risiken zu begegnen, und sollten zu gegebener Zeit entsprechende Mitteilungen herausgeben. Richtet die federführende Überwachungsbehörde Empfehlungen an kritische IKT-Drittdienstleister, die gemäß der Richtlinie (EU) 2022/2555 beaufsichtigt werden, so sollten die zuständigen Behörden auf freiwilliger Basis und vor dem Erlass zusätzlicher Maßnahmen die gemäß der genannten Richtlinie zuständigen Behörden konsultieren können, um einen koordinierten Ansatz in Bezug auf die betreffenden kritischen IKT-Drittdienstleister zu erleichtern.

(91) Die Ausübung der Überwachung sollte sich an drei Handlungsgrundsätzen orientieren, um Folgendes sicherzustellen: a) eine enge Koordinierung zwischen den ESA bei ihren Aufgaben als federführende Überwachungsbehörde mithilfe eines gemeinsamen Überwachungsnetzes (JON — Joint Oversight Network), b) die Kohärenz mit dem durch die Richtlinie (EU) 2022/2555 geschaffenen Rahmen (über eine freiwillige Konsultation der Einrichtungen, die in den Geltungsbereich der genannten Richtlinie fallen, um Doppelarbeit bei an kritische IKT-Drittdienstleister gerichteten Maßnahmen zu vermeiden) und c) eine Sorgfaltspflicht, wonach das potenzielle Risiko einer Störung der von kritischen IKT-Drittdienstleistern bereitgestellten Dienste für Kunden, bei denen es sich um nicht in den Geltungsbereich dieser Verordnung fallende Unternehmen handelt, zu minimieren ist.

(92) Der Überwachungsrahmen sollte nicht die Anforderung an Finanzunternehmen ersetzen, die Risiken, die die Nutzung von IKT-Drittdienstleistern mit sich bringt, selbst zu managen und sollte weder in irgendeiner Form noch für irgendeinen Aspekt an deren Stelle treten; dies schließt auch die Verpflichtung ein, die laufende Überwachung der mit kritischen IKT-Drittdienstleistern geschlossenen vertraglichen Vereinbarungen aufrechtzuerhalten. Ebenso sollte der Überwachungsrahmen die volle Verantwortung der Finanzunternehmen für die Einhaltung und Erfüllung aller Verpflichtungen gemäß dieser Verordnung und dem einschlägigen Finanzdienstleistungsrecht unberührt lassen.

(93) Um Doppelarbeit und Überschneidungen zu vermeiden, sollten die zuständigen Behörden davon absehen, im Alleingang Maßnahmen zur Überwachung des von kritischen IKT-Drittdienstleistern ausgehenden Risikos zu ergreifen, und sollten sich diesbezüglich auf die einschlägige Bewertung der federführenden Überwachungsbehörde stützen. Sämtliche Maßnahmen sollten in jedem Fall zuvor mit der federführenden Überwachungsbehörde im Rahmen der Ausübung ihrer Aufgaben innerhalb des Überwachungsrahmens koordiniert und vereinbart werden.

(94) Um auf internationaler Ebene die Konvergenz in Bezug auf bewährte Verfahren zu fördern, die für die Überprüfung und Überwachung des Managements von IKT-Drittdienstleistern ausgehender digitaler Risiken zu nutzen sind, sollten die ESA aufgefordert werden, Kooperationsvereinbarungen mit den zuständigen Aufsichts- und Regulierungsbehörden in Drittländern zu schließen.

(95) Um die speziellen Qualifikationen, die technischen Kompetenzen und das Fachwissen des auf operationelle und IKT-Risiken spezialisierten Personals innerhalb der zuständigen Behörden, der drei ESA und — auf freiwilliger Basis — der gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden zu nutzen, sollte die federführende Überwachungsbehörde auf nationale Aufsichtsfähigkeiten und das entsprechende Fachwissen zurückgreifen und für jeden einzelnen kritischen IKT-Drittdienstleister spezielle Untersuchungsteams einrichten und multidisziplinäre Teams zusammenlegen, um sowohl die Vorbereitung als auch die tatsächliche Wahrnehmung von Überwachungstätigkeiten zu unterstützen, einschließlich allgemeiner Untersuchungen und Inspektionen kritischer IKT-Drittdienstleister sowie jeglicher erforderlichen Folgemaßnahmen.

(96) Während die Kosten, die sich aus den Überwachungsaufgaben ergeben, vollständig aus Gebühren finanziert würden, die von kritischen IKT-Drittdienstleistern erhoben werden, dürften den ESA hingegen vor Beginn des Überwachungsrahmens Kosten für die Einführung spezieller IKT-Systeme zur Unterstützung der anstehenden Überwachung entstehen, da im Vorfeld spezielle IKT-Systeme entwickelt und eingeführt werden müssten. Diese Verordnung sieht daher ein hybrides Finanzierungsmodell vor, bei dem der Überwachungsrahmen als solcher vollständig gebührenfinanziert wäre, während die Entwicklung der IKT-Systeme der ESA aus Beiträgen der Union und der zuständigen nationalen Behörden finanziert würde.

(97) Zuständige Behörden sollten über alle erforderlichen Aufsichts-, Untersuchungs- und Sanktionsbefugnisse verfügen, um die angemessene Wahrnehmung ihrer Aufgaben im Rahmen dieser Verordnung sicherzustellen. Sie sollten grundsätzlich die von ihnen verhängten Verwaltungssanktionen öffentlich bekannt machen. Da Finanzunternehmen und kritische IKT-Drittdienstleister in unterschiedlichen Mitgliedstaaten ansässig sein und der Aufsicht unterschiedlicher zuständiger Behörden unterliegen können, sollte die Anwendung dieser Verordnung zum einen durch die enge Zusammenarbeit zwischen den jeweils zuständigen Behörden, einschließlich der EZB bei der Wahrnehmung der ihr durch die Verordnung (EU) Nr. 1024/2013 übertragenen besonderen Aufgaben, erleichtert werden sowie zum anderen durch die Abstimmung mit den ESA im Wege des gegenseitigen Informationsaustauschs und der Erbringung von Amtshilfe in den einschlägigen Aufsichtsbelangen.

(98) Um die Kriterien für die Einstufung von IKT-Drittdienstleistern als kritisch weiter zu quantifizieren und zu präzisieren und um Überwachungsgebühren zu harmonisieren, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Verordnung in Bezug auf Folgendes zu erlassen: die weitere Präzisierung der systemischen Auswirkungen, die ein Ausfall eines Dienstes oder ein operativer Ausfall eines IKT-Drittdienstleisters auf die Finanzunternehmen haben könnte, für die er IKT-Dienstleistungen bereitstellt; die Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI), die auf den betreffenden IKT-Drittdienstleister angewiesen sind; die Zahl der IKT-Drittdienstleister, die auf einem bestimmten Markt tätig sind; die Kosten für die Migration von Daten und IKT-Arbeitslasten zu anderen IKT-Drittdienstleistern; sowie den Betrag der Überwachungsgebühren und die damit verbundene Zahlungsweise. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([22]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, sollten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten erhalten, und ihre Sachverständigen sollten systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission haben, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(99) Die kohärente Harmonisierung der in dieser Verordnung festgelegten Anforderungen sollte durch technische Regulierungsstandards gewährleistet werden. In ihrer Funktion als Stellen, die über hochspezialisierte Fachkräfte verfügen, sollten die ESA Entwürfe technischer Regulierungsstandards ausarbeiten, die keine politischen Entscheidungen erfordern, und sie der Kommission vorlegen. In den Bereichen IKT-Risikomanagement, Meldung schwerwiegender IKT-bezogener Vorfälle, Tests sowie in Bezug auf Schlüsselanforderungen für eine solide Überwachung des IKT-Drittparteienrisikos sollten technische Regulierungsstandards entwickelt werden. Die Kommission und die ESA sollten sicherstellen, dass diese Standards und Anforderungen von allen Finanzunternehmen auf eine Weise angewandt werden können, die ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte angemessen ist. Der Kommission sollte die Befugnis übertragen werden, diese technischen Regulierungsstandards mittels delegierter Rechtsakten gemäß Artikel 290 AEUV und im Einklang mit den Artikeln 10 und 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

(100) Um die Vergleichbarkeit der Meldungen über schwerwiegende IKT-bezogene Vorfälle und schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle zu erleichtern sowie um für Transparenz in Bezug auf vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen von Drittdienstleistern zu sorgen, sollten die ESA Entwürfe technischer Durchführungsstandards erarbeiten, mit denen standardisierte Vorlagen, Formulare und Verfahren für Finanzunternehmen zur Meldung schwerwiegender IKT-bezogener Vorfälle und schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle sowie standardisierte Vorlagen für das Informationsregister festgelegt werden. Bei der Ausarbeitung dieser Standards sollten die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte berücksichtigen. Der Kommission sollte die Befugnis übertragen werden, diese technischen Durchführungsstandards mittels Durchführungsrechtsakten gemäß Artikel 291 AEUV und im Einklang mit Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

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

(101) Da weitere Anforderungen bereits durch delegierte Rechtsakte und Durchführungsrechtsakte auf der Grundlage technischer Regulierungs- und Durchführungsstandards in den Verordnungen (EG) Nr. 1060/2009 ([23]), (EU) Nr. 648/2012 ([24]), (EU) Nr. 600/2014 ([25]) bzw. (EU) Nr. 909/2014 ([26]) des Europäischen Parlaments und des Rates festgelegt wurden, ist es angezeigt, die ESA entweder einzeln oder gemeinsam über den Gemeinsamen Ausschuss zu beauftragen, der Kommission technische Regulierungs- und Durchführungsstandards für den Erlass von delegierten Rechtsakten und Durchführungsrechtsakten zur Übernahme und Aktualisierung bestehender IKT-Risikomanagementvorschriften vorzulegen.

(102) Da die vorliegende Verordnung in Verbindung mit der Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates ([27]) eine Konsolidierung der Bestimmungen über IKT-Risikomanagement mit sich bringt, die sich über mehrere Verordnungen und Richtlinien des Besitzstands der Union im Bereich der Finanzdienstleistungen erstrecken, einschließlich der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 und der Verordnung (EU) 2016/1011 ([28]) des Europäischen Parlaments und des Rates, sollten diese Verordnungen zur Gewährleistung vollständiger Übereinstimmung geändert werden, damit klargestellt ist, dass die geltenden Bestimmungen über IKT-Risiken in der vorliegenden Verordnung verankert sind.

(103) Der Geltungsbereich der einschlägigen Artikel über operationelle Risiken, auf deren Grundlage durch Befugnisübertragungen gemäß den Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 (EU) Nr. 909/2014 und (EU) 2016/1011 der Erlass von delegierten Rechtsakten und Durchführungsrechtsakten ermöglicht wurde, sollte folglich eingeschränkt werden, damit alle Bestimmungen, die Aspekte der digitalen operationalen Resilienz betreffen und heute Teil der genannten Verordnungen sind, in die vorliegende Verordnung übernommen werden können.

(104) Das potenzielle systemische Cyberrisiko, das mit der Nutzung von IKT-Infrastrukturen verbunden ist, die den Betrieb von Zahlungssystemen und die Erbringung von Zahlungsabwicklungstätigkeiten ermöglichen, sollte auf Unionsebene durch harmonisierte Vorschriften für die digitale Resilienz angemessen angegangen werden. Zu diesem Zweck sollte die Kommission rasch prüfen, ob der Geltungsbereich der vorliegenden Verordnung überprüft werden muss, und diese Überprüfung zugleich an die Ergebnisse der in der Richtlinie (EU) 2015/2366 vorgesehenen umfassenden Überprüfung anpassen. Zahlreiche Großangriffe in den letzten zehn Jahren haben gezeigt, inwiefern Zahlungssysteme Cyberbedrohungen ausgesetzt sind. Da sie im Mittelpunkt der Zahlungsdienstleistungskette stehen und starke Verflechtungen mit dem gesamten Finanzsystem aufweisen, sind Zahlungssysteme und Zahlungsabwicklungstätigkeiten nunmehr zu einem maßgeblichen Faktor für das Funktionieren der Finanzmärkte der Union geworden. Cyberangriffe auf diese Systeme können zu schwerwiegenden Betriebsstörungen führen, die sich direkt auf wirtschaftliche Schlüsselfunktionen wie die Erleichterung von Zahlungen auswirken und zugleich indirekt Konsequenzen für die damit verbundenen wirtschaftlichen Prozesse haben. Bis zur Einführung eines harmonisierten Systems und der Beaufsichtigung der Betreiber von Zahlungssystemen und Zahlungsabwicklungsunternehmen auf Unionsebene können sich die Mitgliedstaaten zur Anwendung ähnlicher Marktpraktiken an den mit dieser Verordnung festgelegten Anforderungen an die digitale operationale Resilienz orientieren, wenn sie für Betreiber von Zahlungssystemen und Zahlungsabwicklungsunternehmen, die in ihrem jeweiligen Hoheitsgebiet der Aufsicht unterliegen, diesbezügliche Vorschriften anwenden.

---

([23]) Verordnung (EG) Nr. 1060/2009 des Europäischen Parlaments und des Rates vom 16. September 2009 über Ratingagenturen (ABl. L 302 vom 17.11.2009, S. 1).

([24]) 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).

([25]) Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 173 vom 12.6.2014, S. 84).

([26]) Verordnung (EU) Nr. 909/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 zur Verbesserung der Wertpapierlieferungen und -abrechnungen in der Europäischen Union und über Zentralverwahrer sowie zur Änderung der Richtlinien 98/26/EG und 2014/65/EU und der Verordnung (EU) Nr. 236/2012 (ABl. L 257 vom 28.8.2014, S. 1).

([27]) Richtlinie (EU) 2022/2556 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor (siehe Seite 153 dieses Amtsblatts).

([28]) Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über Indizes, die bei Finanzinstrumenten und Finanzkontrakten als Referenzwert oder zur Messung der Wertentwicklung eines Investmentfonds verwendet werden, und zur Änderung der Richtlinien 2008/48/EG und 2014/17/EU sowie der Verordnung (EU) Nr. 596/2014 (ABl. L 171 vom 29.6.2016, S. 1).

(105) Da das Ziel dieser Verordnung, nämlich die Erreichung eines hohen Niveaus an digitaler operationaler Resilienz in beaufsichtigten Finanzunternehmen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, weil es der Harmonisierung einiger unterschiedlicher Vorschriften im Unionsrecht und im nationalen Recht bedarf, sondern vielmehr wegen seines Umfangs und seiner Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im 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 Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(106) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([29]) konsultiert und hat am 10. Mai 2021 eine Stellungnahme abgegeben ([30]) —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

*KAPITEL I*

## *Allgemeine Bestimmungen*

*Artikel 1*

### Gegenstand

(1) Um ein hohes gemeinsames Niveau an digitaler operationaler Resilienz zu erreichen, werden in dieser Verordnung einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen, wie folgt festgelegt:

a) auf Finanzunternehmen anwendbare Anforderungen in Bezug auf:

   i) Risikomanagement im Bereich der Informations- und Kommunikationstechnologie (IKT);

   ii) Meldung schwerwiegender IKT-bezogener Vorfälle und — auf freiwilliger Basis — erheblicher Cyberbedrohungen an die zuständigen Behörden;

   iii) Meldung schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle durch in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführte Finanzunternehmen an die zuständigen Behörden;

   iv) Tests der digitalen operationalen Resilienz;

   v) Austausch von Informationen und Erkenntnissen in Bezug auf Cyberbedrohungen und Schwachstellen;

   vi) Maßnahmen für das solide Management des IKT-Drittparteienrisikos;

b) Anforderungen in Bezug auf vertragliche Vereinbarungen zwischen IKT-Drittdienstleistern und Finanzunternehmen;

c) Vorschriften über die Einrichtung und Ausführung des Überwachungsrahmens für kritische IKT-Drittdienstleister bei der Erbringung von Dienstleistungen für Finanzunternehmen;

d) Vorschriften über die Zusammenarbeit zwischen zuständigen Behörden und Vorschriften über die Beaufsichtigung und Durchsetzung aller von dieser Verordnung erfassten Sachverhalte durch zuständige Behörden.

(2) In Bezug auf Finanzunternehmen, die gemäß den nationalen Vorschriften zur Umsetzung von Artikel 3 der Richtlinie (EU) 2022/2555 als wesentliche oder wichtige Unternehmen ermittelt wurden, gilt diese Verordnung für die Zwecke von Artikel 4 der genannten Richtlinie als sektorspezifischer Rechtsakt der Union.

(3) Diese Verordnung lässt die Zuständigkeiten der Mitgliedstaaten für grundlegende Funktionen des Staates in Bezug auf die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit im Einklang mit dem Unionsrecht unberührt.

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

([30]) ABl. C 229 vom 15.6.2021, S. 16.

*Artikel 2*

**Geltungsbereich**

(1) Unbeschadet der Absätze 3 und 4 gilt diese Verordnung für folgende Unternehmen:

a) Kreditinstitute,

b) Zahlungsinstitute, einschließlich gemäß der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute,

c) Kontoinformationsdienstleister,

d) E-Geld-Institute, einschließlich gemäß der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute,

e) Wertpapierfirmen,

f) Anbieter von Krypto-Dienstleistungen, die gemäß einer Verordnung des Europäischen Parlaments und des Rates über Märkte von Krypto-Werten und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937 (im Folgenden „Verordnung über Märkte von Krypto-Werten“) zugelassen sind, und Emittenten wertreferenzierter Token,

g) Zentralverwahrer,

h) zentrale Gegenparteien,

i) Handelsplätze,

j) Transaktionsregister,

k) Verwalter alternativer Investmentfonds,

l) Verwaltungsgesellschaften,

m) Datenbereitstellungsdienste,

n) Versicherungs- und Rückversicherungsunternehmen,

o) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,

p) Einrichtungen der betrieblichen Altersversorgung,

q) Ratingagenturen,

r) Administratoren kritischer Referenzwerte,

s) Schwarmfinanzierungsdienstleister,

t) Verbriefungsregister,

u) IKT-Drittdienstleister.

(2) Für die Zwecke dieser Verordnung werden die in Absatz 1 Buchstaben a bis t genannten Unternehmen zusammen als „Finanzunternehmen“ bezeichnet.

(3) Diese Verordnung gilt nicht für:

a) Verwalter alternativer Investmentfonds im Sinne von Artikel 3 Absatz 2 der Richtlinie 2011/61/EU;

b) Versicherungs- und Rückversicherungsunternehmen im Sinne von Artikel 4 der Richtlinie 2009/138/EG;

c) Einrichtungen der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 15 Versorgungsanwärtern betreiben;

d) gemäß den Artikeln 2 und 3 der Richtlinie 2014/65/EU ausgenommene natürliche oder juristische Personen;

e) Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, bei denen es sich um Kleinstunternehmen oder kleine oder mittlere Unternehmen handelt;

f) Postgiroämter im Sinne von Artikel 2 Absatz 5 Nummer 3 der Richtlinie 2013/36/EU.

(4) Die Mitgliedstaaten können die in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU aufgeführten Stellen, die sich in ihrem jeweiligen Hoheitsgebiet befinden, vom Geltungsbereich dieser Verordnung ausnehmen. Macht ein Mitgliedstaat von dieser Möglichkeit Gebrauch, so setzt er die Kommission hiervon sowie von allen nachfolgenden Änderungen in Kenntnis. Die Kommission macht diese Informationen auf ihrer Website oder auf andere leicht zugängliche Weise öffentlich zugänglich.

*Artikel 3*

**Begriffsbestimmungen**

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck:

1. „digitale operationale Resilienz“ die Fähigkeit eines Finanzunternehmens, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten und zu überprüfen, indem es entweder direkt oder indirekt durch Nutzung der von IKT-Drittdienstleistern bereitgestellten Dienste das gesamte Spektrum an IKT-bezogenen Fähigkeiten sicherstellt, die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten, die von einem Finanzunternehmen genutzt werden und die kontinuierliche Erbringung von Finanzdienstleistungen und deren Qualität, einschließlich bei Störungen, unterstützen;

2. „Netzwerk- und Informationssystem“ ein Netz- und Informationssystem im Sinne von Artikel 6 Nummer 1 der Richtlinie (EU) 2022/2555;

3. „IKT-Altsystem“ ein IKT-System, das das Ende seines Lebenszyklus (Ende seiner Lebensdauer) erreicht hat, aus technologischen oder wirtschaftlichen Gründen nicht für Upgrades oder Fehlerbehebungen in Frage kommt oder nicht mehr von seinem Anbieter oder einem IKT-Drittdienstleister unterstützt wird, das allerdings weiterhin genutzt wird und die Funktionen des Finanzunternehmens unterstützt;

4. „Sicherheit von Netzwerk- und Informationssystemen“ die Sicherheit von Netz- und Informationssystemen im Sinne von Artikel 6 Nummer 2 der Richtlinie (EU) 2022/2555;

5. „IKT-Risiko“ jeden vernünftigerweise identifizierbaren Umstand im Zusammenhang mit der Nutzung von Netzwerk- und Informationssystemen, der bei Eintritt durch die damit einhergehenden nachteiligen Auswirkungen im digitalen oder physischen Umfeld die Sicherheit der Netzwerk- und Informationssysteme, jeglicher technologieabhängiger Instrumente oder Prozesse, von Geschäften und Prozessen oder der Bereitstellung von Diensten beeinträchtigen kann.

6. „Informationsasset“ eine Sammlung materieller oder immaterieller Informationen, die geschützt werden sollten;

7. „IKT-Asset“ eine Software oder Hardware in den Netzwerk- und Informationssystemen, die das Finanzunternehmen nutzt;

8. „IKT-bezogener Vorfall“ ein von dem Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, das bzw. die die Sicherheit der Netzwerk- und Informationssysteme beeinträchtigt und nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten oder auf die vom Finanzunternehmen erbrachten Dienstleistungen hat;

9. „zahlungsbezogener Betriebs- oder Sicherheitsvorfall“ ein von den in Artikel 2 Absatz 1 Buchstaben a bis d aufgeführten Finanzunternehmen nicht geplantes Ereignis bzw. eine entsprechende Reihe verbundener Ereignisse, unabhängig davon, ob es sich um IKT-bezogene Vorfälle handelt oder nicht, das bzw. die nachteilige Auswirkungen auf die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit zahlungsbezogener Daten oder auf die vom Finanzunternehmen bereitgestellten zahlungsbezogenen Dienste hat;

10. „schwerwiegender IKT-bezogener Vorfall“ einen IKT-Vorfall, der umfassende nachteilige Auswirkungen auf die Netzwerk- und Informationssysteme hat, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen;

11. „schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfall“ einen zahlungsbezogenen Betriebs- oder Sicherheitsvorfall, der umfassende nachteilige Auswirkungen auf die bereitgestellten zahlungsbezogenen Dienste hat;

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

13. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, deren technische Merkmale darauf hindeuten, dass sie das Potenzial haben könnte, einen schwerwiegenden IKT-bezogenen Vorfall oder einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall zu verursachen;

14. „Cyberangriff“ einen böswilligen IKT-bezogenen Vorfall, der auf den Versuch eines Angreifers zurückgeht, einen Vermögenswert zu zerstören, freizulegen, zu verändern, zu deaktivieren, zu entwenden oder auf unberechtigte Weise auf diesen Vermögenswert zuzugreifen oder ihn auf unberechtigte Weise zu nutzen;

15. „Bedrohungsanalyse“ Informationen, die aggregiert, umgewandelt, analysiert, ausgewertet oder erweitert wurden, um den notwendigen Kontext für die Entscheidungsfindung zu schaffen und ein relevantes und ausreichendes Verständnis für die Abmilderung der Auswirkungen eines IKT-bezogenen Vorfalls oder einer Cyberbedrohung zu ermöglichen, einschließlich der technischen Einzelheiten eines Cyberangriffs, der für den Angriff verantwortlichen Personen und ihres Modus Operandi und ihrer Beweggründe;

16. „Schwachstelle“ eine Schwachstelle, Empfindlichkeit oder Fehlfunktion eines Vermögenswerts, eines Systems, eines Prozesses oder einer Kontrolle, die ausgenutzt werden kann;

17. „bedrohungsorientierte Penetrationstests (TLPT — Threat-Led Penetration Testing)“ einen Rahmen, der Taktik, Techniken und Verfahren realer Angreifer, die als echte Cyberbedrohung empfunden werden, nachbildet und einen kontrollierten, maßgeschneiderten, erkenntnisgestützten (Red-Team-) Test der kritischen Live-Produktionssysteme des Finanzunternehmens ermöglicht;

18. „IKT-Drittparteienrisiko“ ein IKT-bezogenes Risiko, das für ein Finanzunternehmen im Zusammenhang mit dessen Nutzung von IKT-Dienstleistungen entstehen kann, die von IKT-Drittdienstleistern oder deren Unterauftragnehmern, einschließlich über Vereinbarungen zur Auslagerung, bereitgestellt werden;

19. „IKT-Drittdienstleister“ ein Unternehmen, das IKT-Dienstleistungen bereitstellt;

20. „gruppeninterner IKT-Dienstleister“ ein Unternehmen, das Teil einer Finanzgruppe ist und überwiegend IKT-Dienstleistungen für Finanzunternehmen derselben Gruppe oder für Finanzunternehmen, die demselben institutsbezogenen Sicherungssystem angehören, bereitstellt, einschließlich deren Mutterunternehmen, Tochterunternehmen und Zweigniederlassungen oder anderer Unternehmen, die in gemeinsamem Eigentum oder unter gemeinsamer Kontrolle stehen;

21. „IKT-Dienstleistungen“ digitale Dienste und Datendienste, die über IKT-Systeme einem oder mehreren internen oder externen Nutzern dauerhaft bereitgestellt werden, einschließlich Hardware als Dienstleistung und Hardwaredienstleistungen, wozu auch technische Unterstützung durch den Hardwareanbieter mittels Software- oder Firmware-Aktualisierungen gehört, mit Ausnahme herkömmlicher analoger Telefondienste;

22. „kritische oder wichtige Funktion“ eine Funktion, deren Ausfall die finanzielle Leistungsfähigkeit eines Finanzunternehmens oder die Solidität oder Fortführung seiner Geschäftstätigkeiten und Dienstleistungen erheblich beeinträchtigen würde oder deren unterbrochene, fehlerhafte oder unterbliebene Leistung die fortdauernde Einhaltung der Zulassungsbedingungen und -verpflichtungen eines Finanzunternehmens oder seiner sonstigen Verpflichtungen nach dem anwendbaren Finanzdienstleistungsrecht erheblich beeinträchtigen würde;

23. „kritischer IKT-Drittdienstleister“ einen IKT-Drittdienstleister, der gemäß Artikel 31 als kritisch eingestuft wurde;

24. „IKT-Drittdienstleister mit Sitz in einem Drittland“ einen IKT-Drittdienstleister, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die mit einem Finanzunternehmen eine vertragliche Vereinbarung über die Bereitstellung von IKT-Dienstleistungen geschlossen hat;

25. „Tochterunternehmen“ ein Tochterunternehmen im Sinne von Artikel 2 Nummer 10 und Artikel 22 der Richtlinie 2013/34/EU;

26. „Gruppe“ eine Gruppe im Sinne von Artikel 2 Nummer 11 der Richtlinie 2013/34/EU;

27. „Mutterunternehmen“ ein Mutterunternehmen im Sinne von Artikel 2 Nummer 9 und Artikel 22 der Richtlinie 2013/34/EU;

28. „IKT-Unterauftragnehmer mit Sitz in einem Drittland“ einen IKT-Unterauftragnehmer, bei dem es sich um eine in einem Drittland niedergelassene juristische Person handelt, die mit einem IKT-Drittdienstleister oder einem IKT-Drittdienstleister mit Sitz in einem Drittland eine vertragliche Vereinbarung geschlossen hat;

29. „IKT-Konzentrationsrisiko“ die Exposition gegenüber einzelnen oder mehreren verbundenen kritischen IKT-Drittdienstleistern, die zu einer gewissen Abhängigkeit von diesen Dienstleistern führt, sodass die Nichtverfügbarkeit, der Ausfall oder sonstige Defizite dieser Dienstleister die Fähigkeit eines Finanzunternehmens gefährden könnten, kritische oder wichtige Funktionen zu erfüllen, oder bei dem Finanzunternehmen andere Formen nachteiliger Auswirkungen, einschließlich großer Verluste, herbeiführen oder die finanzielle Stabilität der Union insgesamt gefährden könnten;

30. „Leitungsorgan“ ein Leitungsorgan im Sinne von Artikel 4 Absatz 1 Nummer 36 der Richtlinie 2014/65/EU, von Artikel 3 Absatz 1 Nummer 7 der Richtlinie 2013/36/EU, von Artikel 2 Absatz 1 Buchstabe s der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates ([31]), von Artikel 2 Absatz 1 Nummer 45 der Verordnung (EU) Nr. 909/2014, von Artikel 3 Absatz 1 Nummer 20 der Verordnung (EU) 2016/1011 sowie im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten oder die entsprechenden Personen, die das Unternehmen tatsächlich leiten oder im Einklang mit dem einschlägigen Unionsrecht oder nationalen Recht Schlüsselfunktionen wahrnehmen;

31. „Kreditinstitut“ ein Kreditinstitut im Sinne von Artikel 4 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([32]);

32. „nach der Richtlinie 2013/36/EU ausgenommenes Institut“ eine in Artikel 2 Absatz 5 Nummern 4 bis 23 der Richtlinie 2013/36/EU aufgeführte Einrichtung;

33. „Wertpapierfirma“ eine Wertpapierfirma im Sinne von Artikel 4 Absatz 1 Nummer 1 der Richtlinie 2014/65/EU;

34. „kleine und nicht verflochtene Wertpapierfirma“ eine Wertpapierfirma, die die in Artikel 12 Absatz 1 der Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates ([33]) genannten Bedingungen erfüllt;

35. „Zahlungsinstitut“ ein Zahlungsinstitut im Sinne von Artikel 4 Nummer 4 der Richtlinie (EU) 2015/2366;

36. „nach der Richtlinie (EU) 2015/2366 ausgenommenes Zahlungsinstitut“ ein Zahlungsinstitut, für das eine Ausnahme nach Artikel 32 Absatz 1 der Richtlinie (EU) 2015/2366 gilt;

37. „Kontoinformationsdienstleister“ einen Kontoinformationsdienstleister im Sinne von Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366;

38. „E-Geld-Institut“ ein E-Geld-Institut im Sinne von Artikel 2 Nummer 1 der Richtlinie 2009/110/EG;

39. „nach der Richtlinie 2009/110/EG ausgenommenes E-Geld-Institut“ ein E-Geld-Institut, für das eine Ausnahme nach Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt;

40. „zentrale Gegenpartei“ eine zentrale Gegenpartei im Sinne von Artikel 2 Nummer 1 der Verordnung (EU) Nr. 648/2012;

41. „Transaktionsregister“ ein Transaktionsregister im Sinne von Artikel 2 Nummer 2 der Verordnung (EU) Nr. 648/2012;

42. „Zentralverwahrer“ ein Zentralverwahrer im Sinne von Artikel 2 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 909/2014;

43. „Handelsplatz“ einen Handelsplatz im Sinne von Artikel 4 Absatz 1 Nummer 24 der Richtlinie 2014/65/EU.

44. „Verwalter alternativer Investmentfonds“ einen Verwalter alternativer Investmentfonds im Sinne von Artikel 4 Absatz 1 Buchstabe b der Richtlinie 2011/61/EU;

45. „Verwaltungsgesellschaft“ eine Verwaltungsgesellschaft im Sinne von Artikel 2 Absatz 1 Buchstabe b der Richtlinie 2009/65/EG.

46. „Datenbereitstellungsdienst“ einen in Artikel 2 Absatz 1 Nummern 34 bis 36 der Verordnung (EU) Nr. 600/2014 genannten Datenbereitstellungsdienst im Sinne der genannten Verordnung;

47. „Versicherungsunternehmen“ ein Versicherungsunternehmen im Sinne von Artikel 13 Nummer 1 der Richtlinie 2009/138/EG;

48. „Rückversicherungsunternehmen“ ein Rückversicherungsunternehmen im Sinne von Artikel 13 Nummer 4 der Richtlinie 2009/138/EG;

---

([31]) Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. L 302 vom 17.11.2009, S. 32).

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

([33]) Verordnung (EU) 2019/2033 des Europäischen Parlaments und des Rates vom 27. November 2019 über Aufsichtsanforderungen an Wertpapierfirmen und zur Änderung der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 575/2013, (EU) Nr. 600/2014 und (EU) Nr. 806/2014 (ABl. L 314 vom 5.12.2019, S. 1).

49. „Versicherungsvermittler“ einen Versicherungsvermittler im Sinne von Artikel 2 Absatz 1 Nummer 3 der Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates ([34]);

50. „Versicherungsvermittler in Nebentätigkeit“ einen Versicherungsvermittler in Nebentätigkeit im Sinne von Artikel 2 Absatz 1 Nummer 4 der Richtlinie (EU) 2016/97;

51. „Rückversicherungsvermittler“ einen Rückversicherungsvermittler im Sinne von Artikel 2 Absatz 1 Nummer 5 der Richtlinie (EU) 2016/97;

52. „Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung im Sinne von Artikel 6 Nummer 1 der Richtlinie (EU) 2016/2341;

53. „kleine Einrichtung der betrieblichen Altersversorgung“ eine Einrichtung der betrieblichen Altersversorgung, die Altersversorgungssysteme mit insgesamt weniger als 100 Versorgungsanwärtern betreibt;

54. „Ratingagentur“ eine Ratingagentur im Sinne von Artikel 3 Absatz 1 Buchstabe b der Verordnung (EG) Nr. 1060/2009;

55. „Anbieter von Krypto-Dienstleistungen“ einen Anbieter von Krypto-Dienstleistungen im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten;

56. „Emittent wertreferenzierter Token“ einen Emittenten „wertreferenzierter Token“ im Sinne der einschlägigen Vorschrift der Verordnung über Märkte von Krypto-Werten;

57. „Administrator kritischer Referenzwerte“ einen Administrator „kritischer Referenzwerte“ im Sinne von Artikel 3 Absatz 1 Nummer 25 der Verordnung (EU) 2016/1011;

58. „Schwarmfinanzierungsdienstleister“ einen Schwarmfinanzierungsdienstleister im Sinne von Artikel 2 Absatz 1 Buchstabe e der Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates ([35]);

59. „Verbriefungsregister“ ein Verbriefungsregister im Sinne von Artikel 2 Nummer 23 der Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates ([36]);

60. „Kleinstunternehmen“ ein Finanzunternehmen, bei dem es sich nicht um einen Handelsplatz, eine zentrale Gegenpartei, ein Transaktionsregister oder einen Zentralverwahrer handelt, das weniger als zehn Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR nicht überschreitet;

61. „federführende Überwachungsbehörde“ die gemäß Artikel 31 Absatz 1 Buchstabe b dieser Verordnung benannte Europäische Aufsichtsbehörde;

62. „Gemeinsamer Ausschuss“ den jeweils in Artikel 54 der Verordnung (EU) Nr. 1093/2010, der Verordnung (EU) Nr. 1094/2010 und der Verordnung (EU) Nr. 1095/2010 genannten Ausschuss;

63. „Kleinunternehmen“ ein Finanzunternehmen, das 10 oder mehr, aber weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. -bilanzsumme 2 Mio. EUR überschreitet, nicht jedoch 10 Mio. EUR;

64. „mittleres Unternehmen“ ein Finanzunternehmen, das kein Kleinunternehmen ist, das weniger als 250 Personen beschäftigt und dessen Jahresumsatz 50 Mio. EUR und/oder dessen Jahresbilanzsumme 43 Mio. EUR nicht überschreitet;

65. „staatliche Behörde“ jede staatliche Stelle oder sonstige Stelle der öffentlichen Verwaltung, einschließlich der nationalen Zentralbanken.

---

([34]) Richtlinie (EU) 2016/97 des Europäischen Parlaments und des Rates vom 20. Januar 2016 über Versicherungsvertrieb (ABl. L 26 vom 2.2.2016, S. 19).

([35]) Verordnung (EU) 2020/1503 des Europäischen Parlaments und des Rates vom 7. Oktober 2020 über Europäische Schwarmfinanzierungsdienstleister für Unternehmen und zur Änderung der Verordnung (EU) 2017/1129 und der Richtlinie (EU) 2019/1937 (ABl. L 347 vom 20.10.2020, S. 1).

([36]) Verordnung (EU) 2017/2402 des Europäischen Parlaments und des Rates vom 12. Dezember 2017 zur Festlegung eines allgemeinen Rahmens für Verbriefungen und zur Schaffung eines spezifischen Rahmens für einfache, transparente und standardisierte Verbriefung und zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 648/2012 (ABl. L 347 vom 28.12.2017, S. 35).

*Artikel 4*

**Grundsatz der Verhältnismäßigkeit**

(1) Die Finanzunternehmen wenden die in Kapitel II festgelegten Vorschriften im Einklang mit dem Grundsatz der Verhältnismäßigkeit an, wobei ihrer Größe und ihrem Gesamtrisikoprofil sowie der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte Rechnung zu tragen ist.

(2) Darüber hinaus muss die Anwendung der Kapitel III und IV sowie des Kapitels V Abschnitt I durch die Finanzunternehmen in einem angemessenen Verhältnis zu ihrer Größe und ihrem Gesamtrisikoprofil sowie zu der Art, dem Umfang und der Komplexität ihrer Dienstleistungen, Tätigkeiten und Geschäfte stehen, wie dies in den einschlägigen Vorschriften jener Kapitel ausdrücklich vorgesehen ist.

(3) Bei der Überprüfung der Kohärenz des IKT-Risikomanagementrahmens auf der Grundlage der Berichte, die den zuständigen Behörden gemäß Artikel 6 Absatz 5 und Artikel 16 Absatz 2 auf Anfrage vorgelegt werden, prüfen die zuständigen Behörden die Anwendung des Grundsatzes der Verhältnismäßigkeit durch die Finanzunternehmen.

*KAPITEL II*

***IKT-Risikomanagement***

Abschnitt I

*Artikel 5*

**Governance und Organisation**

(1) Finanzunternehmen verfügen über einen internen Governance- und Kontrollrahmen, der im Einklang mit Artikel 6 Absatz 4 ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Das Leitungsorgan des Finanzunternehmens definiert, genehmigt, überwacht und verantwortet die Umsetzung aller Vorkehrungen im Zusammenhang mit dem IKT-Risikomanagementrahmen nach Artikel 6 Absatz 1.

Für die Zwecke von Unterabsatz 1 gilt Folgendes:

a) Das Leitungsorgan trägt die letztendliche Verantwortung für das Management der IKT-Risiken des Finanzunternehmens;

b) das Leitungsorgan führt Leitlinien ein, die darauf abzielen, hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten aufrechtzuerhalten;

c) das Leitungsorgan legt klare Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen sowie angemessene Governance-Regelungen fest, um eine wirksame und rechtzeitige Kommunikation, Zusammenarbeit und Koordinierung zwischen diesen Funktionen zu gewährleisten;

d) das Leitungsorgan trägt die Gesamtverantwortung für die Festlegung und Genehmigung der Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8, einschließlich der Festlegung der angemessenen Toleranzschwelle für das IKT-Risiko des Finanzunternehmens gemäß Artikel 6 Absatz 8 Buchstabe b;

e) das Leitungsorgan genehmigt, überwacht und überprüft regelmäßig die Umsetzung der in Artikel 11 Absatz 1 genannten IKT-Geschäftsfortführungsleitlinie und der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne, die als eigenständige spezielle Leitlinie, die integraler Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens und seines Reaktions- und Wiederherstellungsplans ist, verabschiedet werden können;

f) das Leitungsorgan genehmigt und überprüft regelmäßig die internen IKT-Revisionspläne des Finanzunternehmens, die IKT-Revision und die daran vorgenommenen wesentlichen Änderungen;

g) das Leitungsorgan weist angemessene Budgetmittel zu und überprüft diese regelmäßig, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht zu werden, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz nach Artikel 13 Absatz 6 sowie IKT-Kompetenzen für alle Mitarbeiter;

h) das Leitungsorgan genehmigt und überprüft regelmäßig die Leitlinie des Finanzunternehmens in Bezug auf Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die von IKT-Drittdienstleistern bereitgestellt werden;

i) das Leitungsorgan richtet auf Unternehmensebene Meldekanäle ein, die es ihm ermöglichen, ordnungsgemäß über Folgendes informiert zu werden:

   i) mit IKT-Drittdienstleistern geschlossene Vereinbarungen über die Nutzung von IKT-Dienstleistungen,

   ii) alle relevanten geplanten wesentlichen Änderungen in Bezug auf die IKT-Drittdienstleister,

   iii) die potenziellen Auswirkungen derartiger Änderungen auf die kritischen oder wichtigen Funktionen, die Gegenstand dieser Vereinbarungen sind, einschließlich einer Zusammenfassung der Risikoanalyse, um die Auswirkungen dieser Änderungen zu bewerten, und zumindest über schwerwiegende IKT-bezogene Vorfälle und deren Auswirkungen sowie über Gegen-, Wiederherstellungs- und Korrekturmaßnahmen.

(3) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, richten eine Funktion ein, um die mit IKT-Drittdienstleistern über die Nutzung von IKT-Dienstleistungen geschlossenen Vereinbarungen zu überwachen, oder benennen ein Mitglied der Geschäftsleitung, das für die Überwachung der damit verbundenen Risikoexposition und die einschlägige Dokumentation verantwortlich ist.

(4) Die Mitglieder des Leitungsorgans des Finanzunternehmens halten ausreichende Kenntnisse und Fähigkeiten aktiv auf dem neuesten Stand — unter anderem indem sie regelmäßig spezielle Schulungen absolvieren — entsprechend den zu managenden IKT-Risiken, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten können.

## Abschnitt II

*Artikel 6*

**IKT-Risikomanagementrahmen**

(1) Finanzunternehmen verfügen über einen soliden, umfassenden und gut dokumentierten IKT-Risikomanagementrahmen, der Teil ihres Gesamtrisikomanagementsystems ist und es ihnen ermöglicht, IKT-Risiken schnell, effizient und umfassend anzugehen und ein hohes Niveau an digitaler operationaler Resilienz zu gewährleisten.

(2) Der IKT-Risikomanagementrahmen umfasst mindestens Strategien, Leit- und Richtlinien, Verfahren sowie IKT-Protokolle und -Tools, die erforderlich sind, um alle Informations- und IKT-Assets, einschließlich Computer-Software, Hardware und Server, ordnungsgemäß und angemessen zu schützen sowie um alle relevanten physischen Komponenten und Infrastrukturen, wie etwa Räumlichkeiten, Rechenzentren und ausgewiesene sensible Bereiche zu schützen, damit der angemessene Schutz aller Informations- und IKT-Assets vor Risiken, einschließlich der Beschädigung und des unbefugten Zugriffs oder der unbefugten Nutzung, gewährleistet ist.

(3) Im Einklang mit ihrem IKT-Risikomanagementrahmen minimieren Finanzunternehmen die Auswirkungen von IKT-Risiken, indem sie geeignete Strategien, Leit- und Richtlinien, Verfahren, IKT-Protokolle und Tools einsetzen. Sie legen den zuständigen Behörden auf Anfrage vollständige und aktuelle Informationen über IKT-Risiken und ihren IKT-Risikomanagementrahmen vor.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, übertragen die Zuständigkeit für das Management und die Überwachung des IKT-Risikos an eine Kontrollfunktion und stellen ein angemessenes Maß an Unabhängigkeit dieser Kontrollfunktion sicher, um Interessenkonflikte zu vermeiden. Die Finanzunternehmen sorgen für eine angemessene Trennung und Unabhängigkeit von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen gemäß dem Modell der drei Verteidigungslinien oder einem internen Modell für Risikomanagement und Kontrolle.

(5) Der IKT-Risikomanagementrahmen wird mindestens einmal jährlich — bzw. im Falle von Kleinstunternehmen regelmäßig — sowie bei Auftreten schwerwiegender IKT-bezogener Vorfälle und nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, dokumentiert und überprüft. Der Rahmen wird auf Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf deren Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

(6) Im Einklang mit dem Revisionsplan des betreffenden Finanzunternehmens ist der IKT-Risikomanagementrahmen von Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, regelmäßig einer internen Revision durch Revisoren zu unterziehen. Diese Revisoren verfügen über ausreichendes Wissen und ausreichende Fähigkeiten und Fachkenntnisse im Bereich IKT-Risiken sowie über eine angemessene Unabhängigkeit. Häufigkeit und Schwerpunkt von IKT-Revisionen sind den IKT-Risiken des Finanzunternehmens entsprechend angemessen.

(7) Auf der Grundlage der Feststellungen aus der Überprüfung der internen Revision legen Finanzunternehmen ein förmliches Follow-up-Verfahren einschließlich Regeln für die rechtzeitige Überprüfung und Auswertung kritischer Erkenntnisse der IKT-Revision fest.

(8) Der IKT-Risikomanagementrahmen umfasst eine Strategie für die digitale operationale Resilienz, in der dargelegt wird, wie der Rahmen umgesetzt wird. Zu diesem Zweck schließt die Strategie für die digitale operationale Resilienz Methoden, um IKT-Risiken anzugehen und spezifische IKT-Ziele zu erreichen, ein, indem

a) erläutert wird, wie der IKT-Risikomanagementrahmen die Geschäftsstrategie und die Ziele des Finanzunternehmens unterstützt;

b) die Risikotoleranzschwelle für IKT-Risiken im Einklang mit der Risikobereitschaft des Finanzunternehmens festgelegt und die Auswirkungsstoleranz mit Blick auf IKT-Störungen untersucht wird;

c) klare Ziele für die Informationssicherheit festgelegt werden, einschließlich der wesentlichen Leistungsindikatoren und der wesentlichen Risikokennzahlen;

d) die IKT-Referenzarchitektur und etwaige Änderungen erläutert werden, die für die Erreichung spezifischer Geschäftsziele erforderlich sind;

e) die verschiedenen Mechanismen dargelegt werden, die eingesetzt wurden, um IKT-bezogene Vorfälle zu erkennen, sich davor zu schützen und daraus entstehende Folgen zu verhindern;

f) der aktuelle Stand bezüglich der digitalen operationalen Resilienz anhand der Anzahl gemeldeter schwerwiegender IKT-Vorfälle und bezüglich der Wirksamkeit von Präventivmaßnahmen dargelegt wird;

g) Tests der digitalen operationalen Resilienz gemäß Kapitel IV dieser Verordnung durchgeführt werden;

h) für IKT-bezogene Vorfälle eine Kommunikationsstrategie dargelegt wird, die gemäß Artikel 14 offengelegt werden muss.

(9) Finanzunternehmen können im Zusammenhang mit der Strategie für die digitale operationale Resilienz nach Absatz 8 eine ganzheitliche Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene festlegen, in der wesentliche Abhängigkeiten von IKT-Drittdienstleistern aufgezeigt und die Gründe für die Nutzung verschiedener IKT-Drittdienstleister erläutert werden.

(10) Finanzunternehmen können die Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten an gruppeninterne oder externe Unternehmen auslagern. Im Falle einer solchen Auslagerung bleibt das Finanzunternehmen weiterhin uneingeschränkt für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen verantwortlich.

*Artikel 7*

**IKT-Systeme, -Protokolle und -Tools**

Um IKT-Risiken zu bewältigen und zu managen, verwenden und unterhalten Finanzunternehmen stets auf dem neuesten Stand zu haltende IKT-Systeme, -Protokolle und -Tools, die

a) dem Umfang von Vorgängen, die die Ausübung ihrer Geschäftstätigkeiten unterstützen, im Einklang mit dem Grundsatz der Verhältnismäßigkeit nach Artikel 4 angemessen sind;

b) zuverlässig sind;

c) mit ausreichenden Kapazitäten ausgestattet sind, um die Daten, die für die Ausführung von Tätigkeiten und die rechtzeitige Erbringung von Dienstleistungen erforderlich sind, genau zu verarbeiten und Auftragsspitzen, Mitteilungen oder Transaktionen auch bei Einführung neuer Technologien bewältigen zu können;

d) technologisch resilient sind, um dem unter angespannten Marktbedingungen oder anderen widrigen Umständen erforderlichen zusätzlichen Bedarf an Informationsverarbeitung angemessen zu begegnen.

*Artikel 8*

**Identifizierung**

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1 ermitteln und klassifizieren Finanzunternehmen alle IKT-gestützten Unternehmensfunktionen, Rollen und Verantwortlichkeiten, die Informations- und IKT-Assets, die diese Funktionen unterstützen, sowie deren Rollen und Abhängigkeiten hinsichtlich der IKT-Risiken und dokumentieren sie angemessen. Finanzunternehmen überprüfen erforderlichenfalls, mindestens jedoch einmal jährlich, ob diese Klassifizierung und jegliche einschlägige Dokumentation angemessen sind.

(2) Finanzunternehmen ermitteln kontinuierlich alle Quellen für IKT-Risiken, insbesondere das Risiko gegenüber und von anderen Finanzunternehmen, und bewerten Cyberbedrohungen und IKT-Schwachstellen, die für ihre IKT-gestützten Geschäftsfunktionen, Informations- und IKT-Assets relevant sind. Finanzunternehmen überprüfen regelmäßig, mindestens jedoch einmal jährlich die sie betreffenden Risikoszenarien.

(3) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, führen bei jeder wesentlichen Änderung der Netzwerk- und Informationssysteminfrastruktur, der Prozesse oder Verfahren, die sich auf ihre IKT-gestützten Unternehmensfunktionen, Informations- oder IKT-Assets auswirken, eine Risikobewertung durch.

(4) Finanzunternehmen ermitteln alle Informations- und IKT-Assets, einschließlich derer an externen Standorten, Netzwerkressourcen und Hardware, und erfassen diejenigen, die als kritisch gelten. Sie erfassen die Konfiguration von Informations- und IKT-Assets sowie die Verbindungen und Interdependenzen zwischen den verschiedenen Informations- und IKT-Assets.

(5) Finanzunternehmen ermitteln und dokumentieren alle Prozesse, die von IKT-Drittdienstleistern abhängen, und ermitteln Vernetzungen mit IKT-Drittdienstleistern, die Dienste zur Unterstützung kritischer oder wichtiger Funktionen bereitstellen.

(6) Für die Zwecke der Absätze 1, 4 und 5 führen Finanzunternehmen entsprechende Inventare, die sie regelmäßig sowie bei jeder wesentlichen Änderung im Sinne von Absatz 3 aktualisieren.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, führen für alle IKT-Altsysteme regelmäßig, mindestens jedoch einmal jährlich und in jedem Fall vor und nach Anschluss von Technologien, Anwendungen oder Systemen eine spezifische Bewertung des IKT-Risikos durch.

*Artikel 9*

**Schutz und Prävention**

(1) Um einen angemessenen Schutz von IKT-Systemen zu gewährleisten und Gegenmaßnahmen zu organisieren, überwachen und kontrollieren Finanzunternehmen kontinuierlich die Sicherheit und das Funktionieren der IKT-Systeme und -Tools und minimieren durch den Einsatz angemessener IKT-Sicherheitstools, -Richtlinien und -Verfahren die Auswirkungen von IKT-Risiken auf IKT-Systeme.

(2) Finanzunternehmen konzipieren, beschaffen und implementieren IKT-Sicherheitsrichtlinien, -verfahren, -protokolle und -Tools, die darauf abzielen, die Resilienz, Kontinuität und Verfügbarkeit von IKT-Systemen, insbesondere jener zur Unterstützung kritischer oder wichtiger Funktionen, zu gewährleisten und hohe Standards in Bezug auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit, von Daten aufrechtzuerhalten, unabhängig davon, ob diese Daten gespeichert sind oder gerade verwendet oder übermittelt werden.

(3) Um die in Absatz 2 genannten Ziele zu erreichen, greifen Finanzunternehmen auf IKT-Lösungen und -Prozesse zurück, die gemäß Artikel 4 angemessen sind. Diese IKT-Lösungen und -Prozesse müssen

a) die Sicherheit der Datenübermittlungsmittel gewährleisten;

b) das Risiko von Datenkorruption oder -verlust, unbefugtem Zugriff und technischen Mängeln, die die Geschäftstätigkeit beeinträchtigen können, minimieren;

c) dem Mangel an Verfügbarkeit, der Beeinträchtigung der Authentizität und Integrität, den Verletzungen der Vertraulichkeit und dem Verlust von Daten vorbeugen;

d) gewährleisten, dass Daten vor Risiken, die beim Datenmanagement entstehen, einschließlich schlechter Verwaltung, verarbeitungsbedingter Risiken und menschlichem Versagen, geschützt werden.

(4) Als Teil des IKT-Risikomanagementrahmens nach Artikel 6 Absatz 1 gilt für Finanzunternehmen Folgendes:

a) Sie erarbeiten und dokumentieren eine Informationssicherheitsleitlinie, in der Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und der Informations- und IKT-Assets, gegebenenfalls einschließlich derjenigen ihrer Kunden, festgelegt sind;

b) sie richten entsprechend einem risikobasierten Ansatz eine solide Struktur für Netzwerk- und Infrastrukturmanagement unter Verwendung angemessener Techniken, Methoden und Protokolle ein, wozu auch die Umsetzung automatisierter Mechanismen zur Isolierung betroffener Informationsassets im Falle von Cyberangriffen gehören kann;

c) sie implementieren Richtlinien, die den physischen oder logischen Zugang zu Informations- und IKT-Assets ausschließlich auf den Umfang beschränken, der für rechtmäßige und zulässige Funktionen und Tätigkeiten erforderlich ist, und legen zu diesem Zweck eine Reihe von Konzepten, Verfahren und Kontrollen fest, die auf Zugangs- und Zugriffsrechte gerichtet sind, und gewährleisten deren gründliche Verwaltung;

d) sie implementieren Konzepte und Protokolle für starke Authentifizierungsmechanismen, die auf einschlägigen Normen und speziellen Kontrollsystemen basieren, sowie Schutzmaßnahmen für kryptografische Schlüssel, wobei Daten auf der Grundlage der Ergebnisse aus genehmigten Datenklassifizierungs- und IKT-Risikobewertungsprozessen verschlüsselt werden;

e) sie implementieren und dokumentieren Richtlinien, Verfahren und Kontrollen für das IKT-Änderungsmanagement, einschließlich Änderungen an Software, Hardware, Firmware-Komponenten, den Systemen oder von Sicherheitsparametern, die auf einem Risikobewertungsansatz basieren und fester Bestandteil des gesamten Änderungsmanagementprozesses des Finanzunternehmens sind, um sicherzustellen, dass alle Änderungen an IKT-Systemen auf kontrollierte Weise erfasst, getestet, bewertet, genehmigt, implementiert und überprüft werden;

f) sie besitzen angemessene und umfassende dokumentierte Richtlinien für Patches und Updates.

Für die Zwecke von Unterabsatz 1 Buchstabe b konzipieren Finanzunternehmen die Infrastruktur für die Netzanbindung und Netzwerkverbindung so, dass sie sofort getrennt oder segmentiert werden kann, damit eine Ansteckung, insbesondere bei miteinander verbundenen Finanzprozessen, minimiert und verhindert wird.

Für die Zwecke von Unterabsatz 1 Buchstabe e wird das Verfahren für das IKT-Änderungsmanagement von zuständigen Leitungsebenen genehmigt und hat spezifische Protokolle.

*Artikel 10*

**Erkennung**

(1) Finanzunternehmen verfügen über Mechanismen, um anomale Aktivitäten im Einklang mit Artikel 17, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, umgehend zu erkennen und potenzielle einzelne wesentliche Schwachstellen zu ermitteln.

Alle in Unterabsatz 1 aufgeführten Erkennungsmechanismen werden gemäß Artikel 25 regelmäßig getestet.

(2) Die in Absatz 1 genannten Erkennungsmechanismen ermöglichen mehrere Kontrollebenen und legen Alarmschwellen und -kriterien fest, um Reaktionsprozesse bei IKT-bezogenen Vorfällen auszulösen und einzuleiten, einschließlich automatischer Warnmechanismen für Mitarbeiter, die für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen zuständig sind.

(3) Finanzunternehmen stellen ausreichende Ressourcen und Kapazitäten bereit, um Nutzeraktivitäten, das Auftreten von IKT-Anomalien und IKT-bezogenen Vorfällen, darunter insbesondere Cyberangriffe, zu überwachen.

(4) Datenbereitstellungsdienste verfügen darüber hinaus über Systeme, mit denen wirksam Handelsauskünfte auf Vollständigkeit geprüft, Lücken und offensichtliche Fehler erkannt und eine Neuübermittlung angefordert werden können.

*Artikel 11*

**Reaktion und Wiederherstellung**

(1) Als Teil des in Artikel 6 Absatz 1 genannten IKT-Risikomanagementrahmens und auf der Grundlage der Identifizierungsanforderungen nach Artikel 8 legen Finanzunternehmen eine umfassende IKT-Geschäftsfortführungsleitlinie fest, die als eigenständige spezielle Leitlinie, die fester Bestandteil der allgemeinen Geschäftsfortführungsleitlinie des Finanzunternehmens ist, verabschiedet werden kann.

(2) Finanzunternehmen implementieren die IKT-Geschäftsfortführungsleitlinie mittels spezieller, angemessener und dokumentierter Regelungen, Pläne, Verfahren und Mechanismen, die darauf abzielen,

a) die Fortführung der kritischen oder wichtigen Funktionen des Finanzunternehmens sicherzustellen;

b) auf alle IKT-bezogenen Vorfälle rasch, angemessen und wirksam zu reagieren und diesen so entgegenzuwirken, dass Schäden begrenzt werden und die Wiederaufnahme von Tätigkeiten und Wiederherstellungsmaßnahmen Vorrang erhalten;

c) unverzüglich spezielle Pläne zu aktivieren, die Eindämmungsmaßnahmen, Prozesse und Technologien für alle Arten IKT-bezogener Vorfälle ermöglichen und weitere Schäden vermeiden, sowie maßgeschneiderte Verfahren zur Reaktion und Wiederherstellung gemäß Artikel 12 zu aktivieren;

d) vorläufige Auswirkungen, Schäden und Verluste einzuschätzen;

e) Kommunikations- und Krisenmanagementmaßnahmen festzulegen, die gewährleisten, dass allen relevanten internen Mitarbeitern und externen Interessenträgern im Sinne von Artikel 14 aktualisierte Informationen übermittelt werden, und die Meldung an die zuständigen Behörden gemäß Artikel 19 sicherstellen.

(3) Finanzunternehmen implementieren als Teil des in Artikel 6 Absatz 1 genannten IKT-Risikomanagementrahmens damit verbundene IKT-Reaktions- und Wiederherstellungspläne, die einer unabhängigen internen Revision zu unterziehen sind, sofern es sich bei dem Finanzunternehmen nicht um ein Kleinstunternehmen handelt.

(4) Finanzunternehmen erstellen, pflegen und testen regelmäßig angemessene IKT-Geschäftsfortführungspläne, insbesondere in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.

(5) Als Teil der allgemeinen Geschäftsfortführungsleitlinie führen Finanzunternehmen eine Business-Impact-Analyse (BIA) der bestehenden Risiken für schwerwiegende Betriebsstörungen durch. Im Rahmen der BIA bewerten Finanzunternehmen die potenziellen Auswirkungen schwerwiegender Betriebsstörungen anhand quantitativer und qualitativer Kriterien, wobei sie gegebenenfalls interne und externe Daten und Szenarioanalysen heranziehen. Dabei werden die Kritikalität der identifizierten und erfassten Unternehmensfunktionen, Unterstützungsprozesse, Abhängigkeiten von Dritten und Informationsassets sowie deren Interdependenzen berücksichtigt. Die Finanzunternehmen stellen sicher, dass IKT-Assets und -Dienste in voller Übereinstimmung mit der BIA konzipiert und genutzt werden, insbesondere wenn es darum geht, die Redundanz aller kritischen Komponenten in angemessener Weise zu gewährleisten.

(6) Im Rahmen ihres umfassenden IKT-Risikomanagements gilt für Finanzunternehmen Folgendes:

a) sie testen bei IKT-Systemen, die alle Funktionen unterstützen, mindestens jährlich sowie im Falle jeglicher wesentlicher Änderungen an IKT-Systemen, die kritische oder wichtige Funktionen unterstützen, die IKT-Geschäftsfortführungspläne sowie die IKT-Reaktions- und Wiederherstellungspläne;

b) sie testen die gemäß Artikel 14 erstellten Krisenkommunikationspläne.

Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, nehmen für die Zwecke von Unterabsatz 1 Buchstabe a Szenarien für Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme, die für die Erfüllung der Verpflichtungen nach Artikel 12 erforderlich sind, in ihre Testpläne auf.

Finanzunternehmen überprüfen ihre IKT-Geschäftsfortführungsleitlinie und ihre IKT-Reaktions- und Wiederherstellungspläne regelmäßig und berücksichtigen dabei die Ergebnisse von Tests, die gemäß Unterabsatz 1 durchgeführt wurden, sowie die Empfehlungen, die sich aus Audits oder aufsichtlichen Überprüfungen ergeben.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, verfügen über eine Krisenmanagementfunktion, die bei Aktivierung ihrer IKT- Geschäftsfortführungspläne oder ihrer IKT-Reaktions- und Wiederherstellungspläne unter anderem klare Verfahren für die Abwicklung interner und externer Krisenkommunikation gemäß Artikel 14 festlegt.

(8) Finanzunternehmen sorgen dafür, dass Aufzeichnungen über die Tätigkeiten vor und während Störungen, wenn ihre IKT-Geschäftsfortführungspläne oder ihre IKT-Reaktions- und Wiederherstellungspläne aktiviert werden, jederzeit eingesehen werden können.

(9) Zentralverwahrer übermitteln den zuständigen Behörden Kopien der Ergebnisse der Tests der IKT-Geschäftsfortführung oder ähnlicher Vorgänge.

(10) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, melden den zuständigen Behörden auf Anfrage die geschätzten aggregierten jährlichen Kosten und Verluste, die durch schwerwiegende IKT-bezogene Vorfälle verursacht wurden.

(11) Gemäß jeweils Artikel 16 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 arbeiten die Europäischen Aufsichtsbehörden (im Folgenden „ESA“) über den Gemeinsamen Ausschuss bis zum 17. Juli 2024 gemeinsame Leitlinien für die Schätzung der aggregierten jährlichen Kosten und Verluste nach Absatz 10 aus.

*Artikel 12*

**Richtlinie und Verfahren zum Backup sowie Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung**

(1) Um die Wiederherstellung von IKT-Systemen und Daten mit minimaler Ausfallzeit sowie begrenzten Störungen und Verlusten als Teil ihres IKT-Risikomanagementrahmens sicherzustellen, entwickeln und dokumentieren Finanzunternehmen:

a) Richtlinien und Verfahren für die Datensicherung, in denen der Umfang der Daten, die der Sicherung unterliegen, und die Mindesthäufigkeit der Sicherung auf der Grundlage der Kritikalität der Informationen oder des Vertraulichkeitsgrads der Daten festgelegt werden;

b) Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden.

(2) Finanzunternehmen richten Datensicherungssysteme ein, die in Übereinstimmung mit den Richtlinien und Verfahren zur Datensicherung sowie den Verfahren und Methoden zur Wiedergewinnung und Wiederherstellung aktiviert werden können. Die Aktivierung von Datensicherungssystemen darf die Sicherheit der Netzwerk- und Informationssysteme oder die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von Daten nicht gefährden. Die Datensicherungsverfahren sowie die Wiedergewinnungs- und Wiederherstellungsverfahren und -methoden sind regelmäßig zu testen.

(3) Bei der Wiedergewinnung gesicherter Daten mithilfe eigener Systeme verwenden Finanzunternehmen IKT-Systeme, die von ihrem Quellsystem physisch und logisch getrennt sind. Die IKT-Systeme müssen sicher vor unbefugtem Zugriff oder IKT-Manipulationen geschützt sein und die rechtzeitige Wiederherstellung von Diensten ermöglichen, wobei erforderlichenfalls Daten- und Systemsicherungen (Backups) zu nutzen sind.

Bei zentralen Gegenparteien ermöglichen die Wiederherstellungspläne die Wiederherstellung aller zum Zeitpunkt der Störung laufenden Transaktionen, damit die zentrale Gegenpartei weiterhin sicher arbeiten und die Abwicklung zum vorgesehenen Zeitpunkt abschließen kann.

Datenbereitstellungsdienste unterhalten zusätzlich angemessene Ressourcen und verfügen über die entsprechenden Sicherungs- und Wiedergewinnungseinrichtungen, damit ihre Dienste jederzeit angeboten und aufrechterhalten werden können.

(4) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, unterhalten redundante IKT-Kapazitäten mit Ressourcen, Fähigkeiten und Funktionen, die für die Deckung des Geschäftsbedarfs ausreichen und angemessen sind. Kleinstunternehmen bewerten auf der Grundlage ihres Risikoprofils, ob diese redundanten IKT-Kapazitäten unterhalten werden müssen.

(5) Zentralverwahrer unterhalten mindestens einen sekundären Verarbeitungsstandort, dessen Ressourcen, Kapazitäten, Funktionen und Personalressourcen angemessen sind, um den Geschäftsbedarf zu decken.

Der sekundäre Verarbeitungsstandort

a) befindet sich in geografischer Entfernung vom primären Verarbeitungsstandort, damit er ein eigenes Risikoprofil aufweist und nicht von dem Ereignis, das sich am primären Standort ereignet hat, betroffen ist;

b) kann die Kontinuität kritischer oder wichtiger, mit dem primären Standort identischer Funktionen gewährleisten oder ein Leistungsniveau bereitstellen, mit dem sichergestellt wird, dass das Finanzunternehmen seine kritischen Vorgänge im Rahmen der Wiederherstellungsziele durchführt;

c) ist für das Personal des Finanzunternehmens unmittelbar zugänglich, damit die Kontinuität kritischer oder wichtiger Funktionen gewährleistet werden kann, falls der primäre Verarbeitungsstandort nicht mehr zur Verfügung steht.

(6) Bei der Festlegung der Vorgaben für die Wiederherstellungszeit und die Wiederherstellungspunkte jeder Funktion berücksichtigen die Finanzunternehmen, ob es sich um eine kritische oder wichtige Funktion handelt, sowie die potenziellen Gesamtauswirkungen auf die Markteffizienz. Mit diesen Zeitvorgaben ist sichergestellt, dass die vereinbarte Dienstleistungsgüte in Extremszenarien erreicht werden.

(7) Bei der Wiederherstellung nach IKT-bezogenen Vorfällen führen Finanzunternehmen die erforderlichen Prüfungen durch, einschließlich jeglicher Mehrfachprüfungen und Abgleiche, um die größtmögliche Datenintegrität sicherzustellen. Diese Prüfungen werden auch bei der Rekonstruktion von Daten externer Interessenträger durchgeführt, um sicherzustellen, dass alle Daten systemübergreifend einheitlich sind.

*Artikel 13*

**Lernprozesse und Weiterentwicklung**

(1) Finanzunternehmen verfügen über Kapazitäten und Personal, um Informationen über Schwachstellen und Cyberbedrohungen, IKT-bezogene Vorfälle, insbesondere Cyberangriffe, zu sammeln und ihre wahrscheinlichen Auswirkungen auf ihre digitale operationale Resilienz zu untersuchen.

(2) Nach Störungen ihrer Haupttätigkeiten infolge schwerwiegender IKT-bezogener Vorfälle sehen Finanzunternehmen nachträgliche Prüfungen IKT-bezogener Vorfälle vor, die die Ursachen für Störungen untersuchen und die erforderlichen Verbesserungen an IKT-Vorgängen oder im Rahmen der in Artikel 11 genannten IKT-Geschäftsfortführungsleitlinie identifizieren.

Finanzunternehmen, die keine Kleinstunternehmen sind, teilen den zuständigen Behörden auf Verlangen die Änderungen mit, die nach der Prüfung IKT-bezogener Vorfälle gemäß Unterabsatz 1 vorgenommen wurden.

Bei den in Unterabsatz 1 genannten nachträglichen Prüfungen IKT-bezogener Vorfälle wird ermittelt, ob die festgelegten Verfahren befolgt und die ergriffenen Maßnahmen wirksam waren, unter anderem in Bezug auf:

a) die Schnelligkeit bei der Reaktion auf Sicherheitswarnungen und bei der Bestimmung der Auswirkungen von IKT-bezogenen Vorfällen und ihrer Schwere;

b) die Qualität und Schnelligkeit bei der Durchführung forensischer Analysen, sofern dies als zweckmäßig erachtet wird;

c) die Wirksamkeit der Eskalation von Vorfällen innerhalb des Finanzunternehmens;

d) die Wirksamkeit interner und externer Kommunikation.

(3) Erkenntnisse aus gemäß den Artikeln 26 und 27 durchgeführten Tests der digitalen operationalen Resilienz und aus realen IKT-bezogenen Vorfällen, insbesondere Cyberangriffen, werden neben Herausforderungen, die sich bei der Aktivierung von IKT- Geschäftsfortführungsplänen und IKT-Reaktions- und Wiederherstellungsplänen ergeben, zusammen mit einschlägigen Informationen, die mit Gegenparteien ausgetauscht und im Rahmen aufsichtlicher Überprüfungen bewertet werden, kontinuierlich ordnungsgemäß in den IKT-Risikobewertungsprozess einbezogen. Diese Erkenntnisse bilden die Grundlage für angemessene Überprüfungen relevanter Komponenten des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1.

(4) Finanzunternehmen überwachen die Wirksamkeit der Umsetzung ihrer Strategie für die digitale operationale Resilienz gemäß Artikel 6 Absatz 8. Dabei erfassen sie die Entwicklung der IKT-Risiken im Zeitverlauf, untersuchen Häufigkeit, Art, Ausmaß und Entwicklung IKT-bezogener Vorfälle, insbesondere Cyberangriffe und deren Muster, um das Ausmaß der IKT-Risiken — insbesondere in Bezug auf kritische oder wichtige Funktionen — zu verstehen und die Cyberreife und die Abwehrbereitschaft des Finanzunternehmens zu verbessern.

(5) Leitende IKT-Mitarbeiter erstatten dem Leitungsorgan mindestens einmal jährlich über die in Absatz 3 genannten Feststellungen Bericht und geben Empfehlungen ab.

(6) Finanzunternehmen entwickeln Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz, die im Rahmen ihrer Programme für die Mitarbeiterschulung obligatorisch sind. Diese Programme und Schulungen gelten für alle Beschäftigten und die Geschäftsleitung und sind so komplex, dass sie deren jeweiligem Aufgabenbereich angemessen sind. Gegebenenfalls nehmen die Finanzunternehmen entsprechend Artikel 30 Absatz 2 Buchstabe i auch IKT-Drittdienstleister in ihre einschlägigen Schulungsprogramme auf.

(7) Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, überwachen einschlägige technologische Entwicklungen fortlaufend — auch um die möglichen Auswirkungen des Einsatzes solcher neuen Technologien auf die Anforderungen an die IKT-Sicherheit und die digitale operationale Resilienz zu verstehen. Sie halten sich über die neuesten Prozesse für das IKT-Risikomanagement auf dem Laufenden, um gegenwärtige oder neue Formen von Cyberangriffen wirksam abzuwehren.

*Artikel 14*

**Kommunikation**

(1) Als Teil des IKT-Risikomanagementrahmens gemäß Artikel 6 Absatz 1 verfügen Finanzunternehmen über Kommunikationspläne, die je nach Sachlage eine verantwortungsbewusste Offenlegung zumindest von schwerwiegenden IKT-bezogenen Vorfällen oder Schwachstellen gegenüber Kunden und anderen Finanzunternehmen sowie der Öffentlichkeit ermöglichen.

(2) Als Teil des IKT-Risikomanagementrahmens setzen Finanzunternehmen Kommunikationsstrategien für interne Mitarbeiter und externe Interessenträger um. Bei Kommunikationsleitlinien für Mitarbeiter wird berücksichtigt, dass zwischen dem Personal, das am IKT-Risikomanagement, insbesondere im Bereich Reaktion und Wiederherstellung, beteiligt ist, und dem zu informierendem Personal unterschieden werden muss.

(3) Mindestens eine Person im Finanzunternehmen ist mit der Umsetzung der Kommunikationsstrategie für IKT-bezogene Vorfälle beauftragt und nimmt zu diesem Zweck die entsprechende Aufgabe gegenüber der Öffentlichkeit und den Medien wahr.

*Artikel 15*

**Weitere Harmonisierung von Tools, Methoden, Prozessen und Richtlinien für IKT-Risikomanagement**

Die ESA entwickeln über den Gemeinsamen Ausschuss in Abstimmung mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) gemeinsame Entwürfe technischer Regulierungsstandards für folgende Zwecke:

a) die Festlegung weiterer Elemente, die in die in Artikel 9 Absatz 2 genannten Richtlinien, Verfahren, Protokolle und Tools für IKT-Sicherheit aufzunehmen sind, um die Sicherheit von Netzwerken zu gewährleisten, angemessene Schutzvorrichtungen gegen Eindringen und Missbrauch von Daten zu ermöglichen, die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten, einschließlich kryptografischer Techniken, zu wahren und eine präzise und rasche Datenübermittlung ohne wesentliche Störungen und unangemessene Verzögerungen zu gewährleisten;

b) die Entwicklung weiterer Komponenten der Kontrollen von Zugangs- und Zugriffsrechten gemäß Artikel 9 Absatz 4 Buchstabe c und der damit verbundenen Personalpolitik, mit denen Zugangsrechte, Verfahren für Erteilung und Widerruf von Rechten, die Überwachung anomalen Verhaltens in Bezug auf IKT-Risiken durch angemessene Indikatoren — auch für Netzwerknutzungsmuster, Zeiten, IT-Aktivität und unbekannte Geräte — spezifiziert werden;

c) die Weiterentwicklung der in Artikel 10 Absatz 1 genannten Mechanismen, die eine umgehende Erkennung anomaler Aktivitäten ermöglichen, sowie der in Artikel 10 Absatz 2 genannten Kriterien, die Verfahren für die Erkennung IKT-bezogener Vorfälle und die damit verbundenen Reaktionsprozesse auslösen;

d) die Spezifizierung der in Artikel 11 Absatz 1 genannten Komponenten der IKT-Geschäftsfortführungsleitlinie;

e) die Spezifizierung der Tests von IKT-Geschäftsfortführungsplänen gemäß Artikel 11 Absatz 6, damit bei diesen Tests Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt, und die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle einschlägiger IKT-Drittdienstleister sowie gegebenenfalls die etwaigen politischen Risiken in den Rechtsordnungen in den Ländern und Gebieten der jeweiligen Anbieter gebührend berücksichtigt werden;

f) die Spezifizierung der Komponenten der in Artikel 11 Absatz 3 genannten IKT-Reaktions- und Wiederherstellungspläne;

g) die Spezifizierung von Inhalt und Form des in Artikel 6 Absatz 5 genannten Berichts über die Überprüfung des IKT-Risikomanagementrahmens.

Bei der Entwicklung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte, wobei sie etwaigen Besonderheiten, die sich aus der unterschiedlichen Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren ergeben, gebührend Rechnung tragen.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Absatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

*Artikel 16*

**Vereinfachter IKT-Risikomanagementrahmen**

(1) Artikel 5 bis 15 gelten nicht für kleine und nicht verflochtene Wertpapierfirmen, entsprechend der Richtlinie (EU) 2015/2366 ausgenommene Zahlungsinstitute, entsprechend der Richtlinie 2013/36/EU ausgenommene Institute, für die die Mitgliedstaaten beschlossen haben, nicht von der in Artikel 2 Absatz 4 der vorliegenden Verordnung genannten Möglichkeit Gebrauch zu machen, nach der Richtlinie 2009/110/EG ausgenommene E-Geld-Institute und kleine Einrichtungen der betrieblichen Altersversorgung.

Unbeschadet des Unterabsatzes 1 müssen die in Unterabsatz 1 genannten Stellen

a) einen soliden und dokumentierten IKT-Risikomanagementrahmen errichten und aufrechterhalten, in dem die Mechanismen und Maßnahmen für ein rasches, effizientes und umfassendes Management des IKT-Risikos, einschließlich des Schutzes der einschlägigen physischen Komponenten und Infrastrukturen, detailliert sind;

b) die Sicherheit und das Funktionieren aller IKT-Systeme fortlaufend überwachen;

c) die Auswirkungen von IKT-Risiken minimieren, indem solide, resiliente und aktualisierte IKT-Systeme, -Protokolle und -Tools, die zur Unterstützung der Durchführung ihrer Tätigkeiten und zur Bereitstellung von Diensten angemessen sind, verwendet werden, und in angemessener Weise die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten in den Netzwerk- und Informationssystemen schützen;

d) eine rasche Ermittlung und Aufdeckung der Ursachen von IKT-Risiken und -Anomalien in den Netzwerk- und Informationssystemen sowie eine rasche Handhabung von IKT-Vorfällen ermöglichen;

e) die wesentlichen Abhängigkeiten von IKT-Drittdienstleistern ermitteln;

f) die Kontinuität kritischer oder wichtiger Funktionen durch Geschäftsfortführungspläne sowie Gegen- und Wiederherstellungsmaßnahmen, die zumindest Sicherungs- und Wiedergewinnungsmaßnahmen umfassen, gewährleisten;

g) die unter Buchstabe f genannten Pläne und Maßnahmen sowie die Wirksamkeit der gemäß den Buchstaben a und c durchgeführten Kontrollen regelmäßig testen;

h) gegebenenfalls die relevanten operativen Schlussfolgerungen, die sich aus den Tests gemäß Buchstabe g und der Analyse nach einem Vorfall ergeben, in den IKT-Risikobewertungsprozess einbeziehen und entsprechend dem Bedarf und dem IKT-Risikoprofil Programme zur Sensibilisierung für IKT-Sicherheit sowie Schulungen zur digitalen operationalen Resilienz für Personal und Management entwickeln.

(2) Der in Absatz 1 Unterabsatz 2 Buchstabe a genannte IKT-Risikomanagementrahmen wird regelmäßig und bei Auftreten schwerwiegender IKT-bezogener Vorfälle entsprechend den aufsichtsrechtlichen Anweisungen dokumentiert und überprüft. Der Rahmen wird auf der Grundlage der bei Umsetzung und Überwachung gewonnenen Erkenntnisse kontinuierlich verbessert. Der zuständigen Behörde wird auf Anfrage ein Bericht über die Überprüfung des IKT-Risikomanagementrahmens vorgelegt.

(3) Die ESA entwickeln über den Gemeinsamen Ausschuss in Abstimmung mit der ENISA gemeinsame Entwürfe technischer Regulierungsstandards für die folgenden Zwecke:

a) Spezifizierung der Elemente, die in den in Absatz 1 Unterabsatz 1 Buchstabe a genannten IKT-Risikomanagementrahmen aufzunehmen sind;

b) Spezifizierung der Elemente in Bezug auf Systeme, Protokolle und Tools zur Minimierung der in Absatz 1 Unterabsatz 2 Buchstabe c genannten Auswirkungen von IKT-Risiken, um die Sicherheit der Netzwerke zu gewährleisten, angemessene Schutzvorkehrungen gegen Eindringen und Datenmissbrauch zu ermöglichen und die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten zu wahren;

c) Spezifizierung der Komponenten der in Absatz 1 Unterabsatz 2 Buchstabe f genannten IKT-Geschäftsfortführungspläne;

d) Spezifizierung der Vorschriften über die Tests der Geschäftsfortführungspläne und Gewährleistung der Wirksamkeit der Kontrollen gemäß Absatz 1 Unterabsatz 2 Buchstabe g und Gewährleistung, dass bei diesen Tests Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt, gebührend berücksichtigt werden;

e) nähere Spezifizierung von Inhalt und Form des in Absatz 2 genannten Berichts über die Überprüfung des IKT-Risikomanagementrahmens.

Bei der Entwicklung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte.

Die ESA übermitteln der Kommission die Entwürfe dieser technischen Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

*KAPITEL III*

## *Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle*

*Artikel 17*

### Prozess für die Behandlung IKT-bezogener Vorfälle

(1) Finanzunternehmen bestimmen einen Prozess für die Behandlung IKT-bezogener Vorfälle, richten diese ein und wenden sie an, um IKT-bezogene Vorfälle zu erkennen, zu behandeln und zu melden.

(2) Finanzunternehmen erfassen alle IKT-bezogenen Vorfälle und erheblichen Cyberbedrohungen. Finanzunternehmen richten angemessene Verfahren und Prozesse ein, um die kohärente und integrierte Überwachung, Handhabung und Weiterverfolgung IKT-bezogener Vorfälle zu gewährleisten, um sicherzustellen, dass Ursachen ermittelt, dokumentiert und angegangen werden, um das Auftreten solcher Vorfälle zu verhindern.

(3) Durch den in Absatz 1 genannten Prozess für die Behandlung IKT-bezogener Vorfälle

a) werden Frühwarnindikatoren eingesetzt;

b) werden Verfahren zur Ermittlung, Nachverfolgung, Protokollierung, Kategorisierung und Klassifizierung IKT-bezogener Vorfälle entsprechend ihrer Priorität und Schwere und entsprechend der Kritikalität der betroffenen Dienste entsprechend den in Artikel 18 Absatz 1 genannten Kriterien eingerichtet;

c) werden Funktionen und Zuständigkeiten zugewiesen, die bei verschiedenen Arten von IKT-bezogenen Vorfällen und -Szenarien aktiviert werden müssen;

d) werden gemäß Artikel 14 Pläne für die Kommunikation mit Personal, externen Interessenträgern und Medien sowie für die Benachrichtigung von Kunden, für interne Eskalationsverfahren, einschließlich IKT-bezogener Kundenbeschwerden, und für die Bereitstellung von Informationen an andere Finanzunternehmen, die als Gegenparteien fungieren, ausgearbeitet, je nach Sachlage;

e) wird sichergestellt, dass zumindest schwerwiegende IKT-bezogene Vorfälle der zuständigen höheren Führungsebene gemeldet werden und die Geschäftsleitung informiert wird, wobei die Auswirkungen und Gegenmaßnahmen und zusätzliche Kontrollen erläutert werden, die infolge dieser IKT-bezogenen Vorfälle einzurichten sind;

f) werden Verfahren für Reaktionsmaßnahmen bei IKT-bezogenen Vorfällen eingerichtet, um Auswirkungen zu mindern und sicherzustellen, dass die Dienste zeitnah verfügbar und sicher werden.

*Artikel 18*

**Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen**

(1) Finanzunternehmen klassifizieren IKT-bezogene Vorfälle und bestimmen deren Auswirkungen anhand folgender Kriterien:

a) Anzahl und/oder Relevanz der Kunden oder anderer Gegenparteien im Finanzbereich, die von dem IKT-bezogenen Vorfall betroffen sind, und gegebenenfalls des Werts oder der Anzahl der davon betroffenen Transaktionen und ob der IKT-bezogene Vorfall einen Reputationsschaden verursacht hat;

b) Dauer des IKT-bezogenen Vorfalls, einschließlich der Ausfallzeiten des Dienstes;

c) geografische Ausbreitung der von dem IKT-bezogenen Vorfall betroffenen Gebiete, insbesondere wenn mehr als zwei Mitgliedstaaten betroffen sind;

d) die mit dem IKT-bezogenen Vorfall verbundenen Verfügbarkeits-, Authentizitäts-, Integritäts- oder Vertraulichkeitsverluste von Daten;

e) Kritikalität der betroffenen Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens;

f) wirtschaftliche Auswirkungen — insbesondere direkte und indirekte Kosten und Verluste — des IKT-bezogenen Vorfalls auf absoluter und relativer Basis.

(2) Finanzunternehmen stufen Cyberbedrohungen auf der Grundlage der Kritikalität der risikobehafteten Dienste, einschließlich der Transaktionen und Geschäfte des Finanzunternehmens, der Anzahl und/oder Relevanz der betroffenen Kunden oder Gegenparteien im Finanzbereich und der geografischen Ausbreitung der Risikogebiete als erheblich ein.

(3) Die ESA erarbeiten über den Gemeinsamen Ausschuss in Abstimmung mit der EZB und der ENISA gemeinsame Entwürfe technischer Regulierungsstandards, in denen Folgendes präzisiert wird:

a) die in Absatz 1 genannten Kriterien, einschließlich der Wesentlichkeitsschwellen für die Bestimmung schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle, die der Meldepflicht nach Artikel 19 Absatz 1 unterliegen;

b) die Kriterien, die von den zuständigen Behörden anzuwenden sind, um die Relevanz schwerwiegender IKT-bezogener Vorfälle oder gegebenenfalls schwerwiegender zahlungsbezogener Betriebs- oder Sicherheitsvorfälle für die jeweils zuständigen Behörden in anderen Mitgliedstaaten zu bewerten, sowie die Einzelheiten in den Meldungen über schwerwiegende IKT-bezogene Vorfälle oder gegebenenfalls schwerwiegende zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die anderen zuständigen Behörden gemäß Artikel 19 Absätze 6 und 7 übermittelt werden müssen;

c) die in Absatz 2 genannten Kriterien, einschließlich hoher Wesentlichkeitsschwellen für die Bestimmung erheblicher Cyberbedrohungen.

(4) Bei der Ausarbeitung der in Absatz 3 genannten gemeinsamen Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die in Artikel 4 Absatz 2 genannten Kriterien sowie von der ENISA entwickelte und veröffentlichte internationale Standards, Leitlinien und Spezifikationen, gegebenenfalls einschließlich Spezifikationen für andere Wirtschaftszweige. Für die Zwecke der Anwendung der in Artikel 4 Absatz 2 festgelegten Kriterien berücksichtigen die ESA gebührend, dass Kleinstunternehmen sowie kleine und mittlere Unternehmen ausreichende Ressourcen und Kapazitäten mobilisieren können müssen, um sicherzustellen, dass IKT-bezogene Vorfälle rasch bewältigt werden.

Die ESA übermitteln der Kommission diese allgemeinen Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 3 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

*Artikel 19*

**Meldung schwerwiegender IKT-bezogener Vorfälle und freiwillige Meldung erheblicher Cyberbedrohungen**

(1) Finanzunternehmen melden der nach Artikel 46 jeweils zuständigen Behörde gemäß Absatz 4 schwerwiegende IKT-bezogene Vorfälle.

Unterliegt ein Finanzunternehmen der Aufsicht mehr als einer nach Artikel 46 zuständigen nationalen Behörde, so benennen die Mitgliedstaaten eine einzige zuständige Behörde als einschlägige zuständige Behörde, die für die Wahrnehmung der im vorliegenden Artikel aufgeführten Funktionen und Aufgaben verantwortlich ist.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, melden schwerwiegende IKT-bezogene Vorfälle der gemäß Artikel 4 der Richtlinie 2013/36/EU benannten jeweils zuständigen nationalen Behörde, die diese Meldung unverzüglich an die EZB weiterleitet.

Für die Zwecke von Unterabsatz 1 erstellen Finanzunternehmen nach Erfassung und Analyse aller relevanten Informationen unter Verwendung der in Artikel 20 genannten Vorlage die Erstmeldung und die Meldungen nach Absatz 4 und übermitteln diese der zuständigen Behörde. Falls es aus technischen Gründen nicht möglich ist, die Erstmeldung unter Verwendung der Vorlage zu übermitteln, teilen die Finanzunternehmen dies der zuständigen Behörde auf anderem Wege mit.

Die Erstmeldung und die Meldungen nach Absatz 4 enthalten alle Informationen, die die zuständige Behörde benötigt, um die Signifikanz des schwerwiegenden IKT-bezogenen Vorfalls zu ermitteln und mögliche grenzüberschreitende Auswirkungen zu bewerten.

Unbeschadet der Meldung gemäß Unterabsatz 1 durch das Finanzunternehmen an die jeweils zuständige Behörde können die Mitgliedstaaten zusätzlich festlegen, dass einige oder alle Finanzunternehmen die Erstmeldung und jede Meldung nach Absatz 4 auch den gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden oder Computer-Notfallteams (computer security incident response teams — CSIRT) unter Verwendung der in Artikel 20 genannten Vorlage zur Verfügung stellen müssen.

(2) Finanzunternehmen können der jeweils zuständigen Behörde auf freiwilliger Basis erhebliche Cyberbedrohungen melden, wenn sie der Auffassung sind, dass die Bedrohung für das Finanzsystem, die Dienstnutzer oder die Kunden relevant ist. Die jeweils zuständige Behörde kann derartige Informationen anderen in Absatz 6 genannten einschlägigen Behörden zur Verfügung stellen.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, können erhebliche Cyberbedrohungen auf freiwilliger Basis der gemäß Artikel 4 der Richtlinie 2013/36/EU benannten jeweils zuständigen nationalen Behörde melden, die diese Meldung unverzüglich an die EZB weiterleitet.

Die Mitgliedstaaten können festlegen, dass die Finanzunternehmen, die auf freiwilliger Basis eine Meldung gemäß Unterabsatz 1 vornehmen, diese Meldung auch an die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRT erstatten können.

(3) Wenn ein schwerwiegender IKT-bezogener Vorfall auftritt und Auswirkungen auf die finanziellen Interessen von Kunden hat, unterrichten die Finanzunternehmen, sobald sie hiervon Kenntnis erlangt haben, ihre Kunden unverzüglich über den schwerwiegenden IKT-bezogenen Vorfall und die Maßnahmen, die ergriffen wurden, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern.

Im Falle einer erheblichen Cyberbedrohung unterrichten die Finanzunternehmen gegebenenfalls ihre potenziell betroffenen Kunden über angemessene Schutzmaßnahmen, die diese ergreifen könnten.

(4) Finanzunternehmen legen innerhalb der in Artikel 20 Absatz 1 Buchstabe a Ziffer ii festzulegenden Fristen der jeweils zuständigen Behörde Folgendes vor:

a) eine Erstmeldung;

b) nach der Erstmeldung gemäß Buchstabe a eine Zwischenmeldung, sobald sich der Status des ursprünglichen Vorfalls erheblich geändert hat oder sich die Handhabung des schwerwiegenden IKT-bezogenen Vorfalls auf der Grundlage neuer verfügbarer Informationen geändert hat, gegebenenfalls gefolgt von aktualisierten Meldungen, wann immer eine entsprechende Statusaktualisierung vorliegt, sowie auf ausdrücklichen Antrag der zuständigen Behörde;

c) eine Abschlussmeldung, wenn die Ursachenanalyse abgeschlossen ist — unabhängig davon, ob bereits Minderungsmaßnahmen getroffen wurden oder nicht — und sich die tatsächlichen Auswirkungen beziffern lassen und Schätzungen ersetzen.

(5) Finanzunternehmen dürfen im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten die Meldepflichten nach diesem Artikel an einen Drittdienstleister auslagern. Bei einer solchen Auslagerung bleibt das Finanzunternehmen in vollem Umfang für die Erfüllung der Anforderungen für die Meldung von Vorfällen verantwortlich.

(6) Nach Eingang der Erstmeldung und jeder Meldung nach Absatz 4 übermittelt die zuständige Behörde auf der Grundlage der je nach Sachlage bestehenden jeweiligen Zuständigkeiten zeitnah Einzelheiten zu dem schwerwiegenden IKT-bezogenen Vorfall an die folgenden Empfänger:

a) die EBA, die ESMA oder die EIOPA;

b) die EZB, sofern es sich um Finanzunternehmen im Sinne von Artikel 2 Absatz 1 Buchstaben a, b und d handelt;

c) die zuständigen Behörden, die zentrale Anlaufstelle oder die CSIRT, die jeweils gemäß der Richtlinie (EU) 2022/2555 benannt oder eingerichtet werden;

d) die in Artikel 3 der Richtlinie 2014/59/EU genannten Abwicklungsbehörden und den Einheitlichen Abwicklungsausschuss (Single Resolution Board — SRB) in Bezug auf die in Artikel 7 Absatz 2 der Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates ([37]) genannten Unternehmen sowie in Bezug auf die in Artikel 7 Absatz 4 Buchstabe b und Absatz 5 der Verordnung (EU) Nr. 806/2014 genannten Unternehmen und Gruppen, wenn diese Einzelheiten Vorfälle betreffen, die ein Risiko für die Sicherstellung kritischer Funktionen im Sinne von Artikel 2 Absatz 1 Nummer 35 der Richtlinie 2014/59/EU darstellen; und

e) andere einschlägige Behörden nach nationalem Recht.

(7) Nach Erhalt der Informationen gemäß Absatz 6 bewerten die EBA, die ESMA oder die EIOPA und die EZB in Abstimmung mit der ENISA und in Zusammenarbeit mit der jeweils zuständigen Behörde, ob der schwerwiegende IKT-bezogene Vorfall für die zuständigen Behörden in anderen Mitgliedstaaten von Belang ist. Im Anschluss an diese Bewertung benachrichtigen die EBA, die ESMA oder die EIOPA die jeweils zuständigen Behörden in anderen Mitgliedstaaten entsprechend. Die EZB unterrichtet die Mitglieder des Europäischen Systems der Zentralbanken über die für das Zahlungssystem relevanten Aspekte. Auf der Grundlage dieser Unterrichtung treffen die zuständigen Behörden gegebenenfalls alle für die unmittelbare Stabilität des Finanzsystems notwendigen Schutzvorkehrungen.

([37]) Verordnung (EU) Nr. 806/2014 des Europäischen Parlaments und des Rates vom 15. Juli 2014 zur Festlegung einheitlicher Vorschriften und eines einheitlichen Verfahrens für die Abwicklung von Kreditinstituten und bestimmten Wertpapierfirmen im Rahmen eines einheitlichen Abwicklungsmechanismus und eines einheitlichen Abwicklungsfonds sowie zur Änderung der Verordnung (EU) Nr. 1093/2010 (ABl. L 225 vom 30.7.2014, S. 1).

(8) Die von der ESMA gemäß Absatz 7 vorzunehmende Meldung berührt nicht die Verantwortung der zuständigen Behörde, die Einzelheiten des schwerwiegenden IKT-bezogenen Vorfalls umgehend an die einschlägige Behörde des Aufnahmemitgliedstaats weiterzuleiten, wenn ein Zentralverwahrer eine umfassende grenzüberschreitende Tätigkeit in dem Aufnahmemitgliedstaat ausübt, der schwerwiegende IKT-bezogene Vorfall wahrscheinlich schwerwiegende Folgen für die Finanzmärkte des Aufnahmemitgliedstaats hat und zwischen den zuständigen Behörden Kooperationsvereinbarungen in Bezug auf die Beaufsichtigung von Finanzunternehmen bestehen.

*Artikel 20*

**Harmonisierung von Inhalt und Vorlagen von Meldungen**

Die ESA erarbeiten über den Gemeinsamen Ausschuss und in Abstimmung mit der ENISA und der EZB

a) gemeinsame Entwürfe technischer Regulierungsstandards, um

   i) den Inhalt von Meldungen über schwerwiegende IKT-bezogene Vorfälle festzulegen, damit den in Artikel 18 Absatz 1 aufgeführten Kriterien Rechnung getragen wird und weitere Elemente einbezogen werden, wie z. B. Einzelheiten zur Feststellung der Relevanz der Meldungen für andere Mitgliedstaaten und die Frage, ob es sich dabei um einen schwerwiegenden zahlungsbezogenen Betriebs- oder Sicherheitsvorfall handelt;

   ii) die Fristen für die Erstmeldung und jede Meldung nach Artikel 19 Absatz 4 festzulegen;

   iii) den Inhalt der Meldung erheblicher Cyberbedrohungen festzulegen.

   Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte, um insbesondere sicherzustellen, dass den Besonderheiten der Finanzsektoren für die Zwecke des vorliegenden Absatzes Buchstabe a Ziffer ii gegebenenfalls durch unterschiedliche Fristen Rechnung getragen wird, unbeschadet der Beibehaltung eines kohärenten Ansatzes für die Meldung IKT-bezogener Vorfälle gemäß dieser Verordnung und gemäß der Richtlinie (EU) 2022/2555. Die ESA legen — sofern zutreffend — eine Begründung vor, wenn sie von den im Rahmen jener Richtlinie verfolgten Ansätzen abweichen;

b) gemeinsame Entwürfe technischer Durchführungsstandards zur Festlegung von Standardformularen, Vorlagen und Verfahren für Finanzunternehmen zur Meldung eines schwerwiegenden IKT-bezogenen Vorfalls oder einer erheblichen Cyberbedrohung.

Die ESA übermitteln der Kommission die in Absatz 1 Buchstabe a genannten gemeinsamen Entwürfe technischer Regulierungsstandards und die in Absatz 1 Buchstabe b genannten gemeinsamen Entwürfe technischer Durchführungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, diese Verordnung durch Annahme der in Absatz 1 Buchstabe a genannten gemeinsamen technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

Der Kommission wird die Befugnis übertragen, die in Absatz 1 Buchstabe b genannten gemeinsamen technischen Durchführungsstandards gemäß Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 (EU) Nr. 1095/2010 zu erlassen.

*Artikel 21*

**Zentralisierung der Berichterstattung über schwerwiegende IKT-bezogene Vorfälle**

(1) Die ESA erstellen über den Gemeinsamen Ausschuss und in Abstimmung mit der EZB und der ENISA einen gemeinsamen Bericht, in dem sie die Durchführbarkeit einer weiteren Zentralisierung der Meldung von Vorfällen durch die Einrichtung einer einheitlichen EU-Plattform für die Meldung schwerwiegender IKT-bezogener Vorfälle durch Finanzunternehmen bewerten. In dem gemeinsamen Bericht werden Möglichkeiten sondiert, um den Meldefluss zu IKT-bezogenen Vorfällen zu erleichtern, damit verbundene Kosten zu senken und thematische Analysen zur Erhöhung aufsichtlicher Konvergenz zu unterstützen.

(2) Der in Absatz 1 genannte gemeinsame Bericht umfasst mindestens die folgenden Aspekte:

a) Voraussetzungen für die Einrichtung einer einheitlichen EU-Plattform;

b) Vorteile, Grenzen und Risiken, einschließlich Risiken im Zusammenhang mit einer hohen Konzentration sensibler Informationen;

c) die erforderliche Fähigkeit zur Gewährleistung der Interoperabilität im Hinblick auf andere einschlägige Meldesysteme;

d) Elemente des Betriebsmanagements;

e) Voraussetzungen für die Mitgliedschaft;

f) technische Regelungen für den Zugang von Finanzunternehmen und zuständigen nationalen Behörden zur einheitlichen EU-Plattform;

g) eine vorläufige Bewertung der finanziellen Kosten, die durch die Einrichtung der operativen Plattform zur Unterstützung der einheitlichen EU-Plattform entstehen, einschließlich des erforderlichen Fachwissens.

(3) Die ESA übermitteln dem Europäischen Parlament, dem Rat und der Kommission den in Absatz 1 genannten Bericht bis zum 17. Januar 2025.

*Artikel 22*

**Rückmeldungen von Aufsichtsbehörden**

(1) Unbeschadet der technischen Informationen, Empfehlungen oder Abhilfe- und Folgemaßnahmen, die im Einklang mit dem nationalen Recht gegebenenfalls vom CSIRT gemäß Richtlinie (EU) 2022/2555 bereitgestellt werden können, bestätigt die zuständige Behörde nach Eingang der Erstmeldung und jeder Meldung nach Artikel 19 Absatz 4 den Eingang und kann, wenn möglich, dem Finanzunternehmen zeitnah sachdienliche und angemessene Rückmeldungen oder allgemein gehaltene Orientierungshilfen übermitteln, insbesondere durch Zurverfügungstellung relevanter anonymisierter Informationen und Erkenntnisse zu ähnlichen Bedrohungen, sowie auf Ebene des Unternehmens angewandte Abhilfemaßnahmen und Möglichkeiten zur Minimierung und Minderung nachteiliger Auswirkungen auf den gesamten Finanzsektor erörtern. Unbeschadet der aufsichtlichen Rückmeldung bleiben Finanzunternehmen in vollem Umfang für die Handhabung und die Folgen der gemäß Artikel 19 Absatz 1 gemeldeten IKT-bezogenen Vorfälle verantwortlich.

(2) Die ESA berichten jährlich über den Gemeinsamen Ausschuss in anonymisierter und aggregierter Form über schwerwiegende IKT-bezogene Vorfälle, deren Einzelheiten von den zuständigen Behörden gemäß Artikel 19 Absatz 6 übermittelt werden, und geben dabei mindestens die Zahl schwerwiegender IKT-bezogener Vorfälle, ihre Art und ihre Auswirkungen auf die Geschäftstätigkeit von Finanzunternehmen oder Kunden sowie die ergriffenen Abhilfemaßnahmen und die Kosten an.

Die ESA geben Warnungen heraus und erstellen allgemein gehaltene Statistiken, um die Bewertungen von Bedrohungen und Schwachstellen im IKT-Bereich zu unterstützen.

*Artikel 23*

**Zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, die Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen**

Die Anforderungen in diesem Kapitel gelten auch für zahlungsbezogene Betriebs- oder Sicherheitsvorfälle, auch schwerwiegender Art, wenn sie Kreditinstitute, Zahlungsinstitute, Kontoinformationsdienstleister und E-Geld-Institute betreffen.

*KAPITEL IV*

## *Testen der digitalen operationalen Resilienz*

*Artikel 24*

### Allgemeine Anforderungen für das Testen der digitalen operationalen Resilienz

(1) Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten, Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, erstellen, pflegen und überprüfen Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien ein solides und umfassendes Programm für das Testen der digitalen operationalen Resilienz als integraler Bestandteil des in Artikel 6 genannten IKT-Risikomanagementrahmens.

(2) Das Programm für Tests der digitalen operationalen Resilienz umfasst eine Reihe von Bewertungen, Tests, Methoden, Verfahren und Tools, die gemäß den Artikeln 25 und 26 anzuwenden sind.

(3) Bei der Ausführung des in Absatz 1 genannten Programms für das Testen der digitalen operationalen Resilienz wenden Finanzunternehmen, die keine Kleinstunternehmen sind, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien einen risikobasierten Ansatz an, wobei sie die sich entwickelnden IKT-Risikolandschaften, etwaige spezifische Risiken, denen das betreffende Finanzunternehmen ausgesetzt ist oder ausgesetzt sein könnte, die Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie alle sonstigen Faktoren, die das Finanzunternehmen für angemessen hält, gebührend berücksichtigen.

(4) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass Tests von unabhängigen, internen oder externen Parteien durchgeführt werden. Werden die Tests von einem internen Tester durchgeführt, stellen die Finanzunternehmen ausreichende Ressourcen bereit und tragen dafür Sorge, dass während der Konzeptions- und Durchführungsphase der Prüfung keine Interessenkonflikte entstehen.

(5) Finanzunternehmen, die keine Kleinstunternehmen sind, legen Verfahren und Leitlinien zur Priorisierung, Klassifizierung und Behebung aller während der Durchführung der Tests zutage getretenen Probleme fest und legen interne Validierungsmethoden fest, um sicherzustellen, dass alle ermittelten Schwächen, Mängel oder Lücken vollständig angegangen werden.

(6) Finanzunternehmen, die keine Kleinstunternehmen sind, stellen sicher, dass bei allen IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, mindestens einmal jährlich angemessene Tests durchgeführt werden.

*Artikel 25*

### Testen von IKT-Tools und -Systemen

(1) Das in Artikel 24 genannte Programm für die Tests der digitalen operationalen Resilienz beinhaltet im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien die Durchführung angemessener Tests, wie etwa Schwachstellenbewertung und -scans, Open-Source-Analysen, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen, Quellcodeprüfungen soweit durchführbar, szenariobasierte Tests, Kompatibilitätstests, Leistungstests, End-to-End-Tests und Penetrationstests.

(2) Zentralverwahrer und zentrale Gegenparteien führen Schwachstellenbewertungen durch, bevor Anwendungen und Infrastrukturkomponenten sowie IKT-Dienstleistungen, die kritische oder wichtige Funktionen des Finanzunternehmens unterstützen, eingesetzt oder wieder eingesetzt werden.

(3) Kleinstunternehmen führen die in Absatz 1 genannten Tests durch, indem sie einen risikobasierten Ansatz mit einer strategischen Planung für IKT-Tests kombinieren, wobei sie gebührend berücksichtigen, dass zwischen dem Umfang von Ressourcen und der Zeit, die für die IKT-Tests gemäß diesem Artikel aufzuwenden sind, einerseits, und der Dringlichkeit, der Art des Risikos, der Kritikalität von Informationsassets und erbrachten Dienstleistungen sowie allen sonstigen relevanten Faktoren, einschließlich der Fähigkeit des Finanzunternehmens, kalkulierte Risiken einzugehen, andererseits, ein ausgewogenes Verhältnis gewahrt werden muss.

*Artikel 26*

**Erweiterte Tests von IKT-Tools, -Systemen und -Prozessen auf Basis von TLPT**

(1) Gemäß Absatz 8 Unterabsatz 3 des vorliegenden Artikels ermittelte Finanzunternehmen, bei denen es sich weder um die in Artikel 16 Absatz 1 Unterabsatz 1 genannten Unternehmen noch um Kleinstunternehmen handelt, führen mindestens alle drei Jahre anhand von TLPT erweiterte Tests durch. Auf der Grundlage des Risikoprofils des Finanzunternehmens und unter Berücksichtigung der betrieblichen Gegebenheiten kann die zuständige Behörde das Finanzunternehmen erforderlichenfalls auffordern, die Häufigkeit dieser Tests zu verringern oder zu erhöhen.

(2) Jeder bedrohungsorientierte Penetrationstest schließt mehrere oder alle kritischen oder wichtigen Funktionen eines Finanzunternehmens ein und wird an Live-Produktionssystemen durchgeführt, die derartige Funktionen unterstützen.

Finanzunternehmen ermitteln alle relevanten zugrunde liegenden IKT-Systeme, -Prozesse und -Technologien, die kritische oder wichtige Funktionen und IKT-Dienstleistungen unterstützen, einschließlich derer, die diejenigen kritischen oder wichtigen Funktionen unterstützen, die an IKT-Drittdienstleister ausgelagert oder per Vertrag vergeben wurden.

Finanzunternehmen bewerten, welche kritischen oder wichtigen Funktionen ein TLPT einschließen muss. Der genaue Umfang von TLPT ist vom Ergebnis dieser Bewertung abhängig und wird von den zuständigen Behörden validiert.

(3) Sind IKT-Drittdienstleister in das Spektrum der TLPT einbezogen, ergreift das Finanzunternehmen alle erforderlichen Maßnahmen und Vorkehrungen, um die Einbindung dieser IKT-Drittdienstleister in die TLPT sicherzustellen, und trägt jederzeit die volle Verantwortung für die Gewährleistung der Einhaltung dieser Verordnung.

(4) Wenn vernünftigerweise davon auszugehen ist, dass sich die Einbindung eines IKT-Drittdienstleisters in einen TLPT gemäß Absatz 3 nachteilig auf die Qualität oder die Sicherheit von Dienstleistungen des IKT-Drittdienstleisters an Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, oder auf die Vertraulichkeit in Bezug auf die mit diesen Dienstleistungen verbundenen Daten auswirkt, können das Finanzunternehmen und der IKT-Drittdienstleister unbeschadet Absatz 2 Unterabsätze 1 und 2 schriftlich vereinbaren, dass der IKT-Drittdienstleister unmittelbar vertragliche Vereinbarungen mit einem externen Tester schließt, um unter der Leitung eines benannten Finanzunternehmens einen gebündelten TLPT durchzuführen, an dem mehrere Finanzunternehmen beteiligt sind (gebündelter Test), für die der IKT-Drittdienstleister IKT-Dienstleistungen erbringt.

Diese gebündelten Tests erstrecken sich auf das relevante Spektrum von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von den Finanzunternehmen per Vertrag an die jeweiligen IKT-Drittdienstleister vergeben wurden. Die gebündelten Tests gelten als TLPT, die von den an den gebündelten Tests beteiligten Finanzunternehmen durchgeführt werden.

Die Zahl der Finanzunternehmen, die sich an den gebündelten Tests beteiligen, wird unter Berücksichtigung der Komplexität und der Art der betreffenden Dienstleistungen angemessen austariert.

(5) Finanzunternehmen wenden in Zusammenarbeit mit IKT-Drittdienstleistern und anderen beteiligten Parteien, einschließlich der Tester, jedoch ohne die zuständigen Behörden, wirksame Risikomanagementkontrollen an, um die Gefahr von potenziellen Auswirkungen auf Daten, Schäden an Vermögenswerten und Unterbrechungen kritischer oder wichtiger Funktionen, Dienste oder Vorgänge im Finanzunternehmen selbst, seinen Gegenparteien oder im Finanzsektor zu mindern.

(6) Nach Abschluss der Tests und der Ausarbeitung von Berichten und Plänen mit Abhilfemaßnahmen legen das Finanzunternehmen und gegebenenfalls die externen Tester der gemäß Absatz 9 oder 10 benannten Behörde eine Zusammenfassung der maßgeblichen Ergebnisse, die Pläne mit Abhilfemaßnahmen und die Unterlagen vor, mit denen belegt wird, dass der TLPT anforderungsgemäß durchgeführt wurden.

(7) Die Behörden stellen Finanzunternehmen eine Bescheinigung aus, aus der hervorgeht, dass der Test — wie in den Unterlagen nachgewiesen — im Einklang mit den Anforderungen durchgeführt wurde, um die gegenseitige Anerkennung bedrohungsorientierter Penetrationstests zwischen den zuständigen Behörden zu ermöglichen. Das Finanzunternehmen übermittelt der jeweils zuständigen Behörde die Bescheinigung, die Zusammenfassung der maßgeblichen Ergebnisse und die Abhilfemaßnahmen.

Unbeschadet einer solchen Bescheinigung bleiben Finanzunternehmen jederzeit in vollem Umfang für die Auswirkungen der in Absatz 4 genannten Tests verantwortlich.

(8) Finanzunternehmen beauftragen Tester für die Zwecke der Durchführung von TLPT gemäß Artikel 27. Ziehen Finanzunternehmen für die Zwecke der Durchführung von TLPT interne Tester heran, so beauftragen sie für jeden dritten Test einen externen Tester.

Kreditinstitute, die gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuft wurden, ziehen nur externe Tester gemäß Artikel 27 Absatz 1 Buchstaben a bis e heran.

Die zuständigen Behörden ermitteln Finanzunternehmen, die TLPT durchzuführen haben, unter Berücksichtigung der in Artikel 4 Absatz 2 aufgeführten Kriterien und stützen sich dabei auf die Bewertung von:

a) wirkungsbezogenen Faktoren, darunter insbesondere inwieweit sich die vom Finanzunternehmen erbrachten Dienstleistungen und ausgeführten Tätigkeiten auf den Finanzsektor auswirken;

b) etwaigen Bedenken hinsichtlich der Finanzstabilität, einschließlich des systemischen Charakters des Finanzunternehmens auf Unionsebene oder auf nationaler Ebene, je nach Sachlage;

c) dem spezifischen IKT-Risikoprofil, dem IKT-Reifegrad des Finanzunternehmens oder einschlägigen technologischen Merkmalen.

(9) Die Mitgliedstaaten können eine einzige staatliche Behörde für den Finanzsektor benennen, die auf nationaler Ebene für mit TLPT verbundenen Angelegenheiten im Finanzsektor zuständig ist, und betrauen sie mit allen diesbezüglichen Zuständigkeiten und Aufgaben.

(10) In Ermangelung einer Benennung gemäß Absatz 9 und unbeschadet der Befugnis zur Ermittlung der Finanzunternehmen, die verpflichtet sind, TLPT durchzuführen, kann eine zuständige Behörde die Wahrnehmung einiger oder aller in diesem Artikel oder in Artikel 27 genannten Aufgaben auf eine andere für den Finanzsektor zuständige nationale Behörde übertragen.

(11) Die ESA arbeiten im Einvernehmen mit der EZB im Einklang mit dem TIBER-EU-Rahmen gemeinsame Entwürfe technischer Regulierungsstandards aus, in denen Folgendes präzisiert wird:

a) die für die Zwecke der Anwendung von Absatz 8 Unterabsatz 2 herangezogenen Kriterien;

b) die Anforderungen und Standards für den Einsatz interner Tester;

c) die Anforderungen hinsichtlich:

   i) des Umfangs der in Absatz 2 genannten TLPT;

   ii) der Testmethodik und des Testkonzepts für jede einzelne Phase des Testverfahrens;

   iii) der Ergebnisse, des Abschlusses und der Behebungsphasen der Tests;

d) der Art der aufsichtlichen und sonstigen relevanten Zusammenarbeit, die für die Umsetzung von TLPT und die Erleichterung der gegenseitigen Anerkennung dieser Tests im Kontext von Finanzunternehmen, die in mehr als einem Mitgliedstaat tätig sind, erforderlich ist, um eine angemessene Beteiligung der Aufsichtsbehörden und eine flexible Umsetzung zu ermöglichen, damit den Besonderheiten finanzieller Teilsektoren oder lokaler Finanzmärkte Rechnung getragen wird.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA gebührend etwaige Besonderheiten, die sich aus der unterschiedlichen Art der Tätigkeiten in verschiedenen Finanzdienstleistungssektoren ergeben.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

*Artikel 27*

**Anforderungen an Tester bezüglich der Durchführung von TLPT**

(1) Finanzunternehmen ziehen für TLPT nur Tester heran, die

a) von höchster Eignung und Ansehen sind;

b) über technische und organisatorische Fähigkeiten verfügen und spezifisches Fachwissen in den Bereichen Bedrohungsanalyse, Penetrationstests und Red-Team-Tests nachweisen;

c) von einer Akkreditierungsstelle in einem Mitgliedstaat zertifiziert wurden oder formale Verhaltenskodizes oder ethische Rahmenregelungen einhalten;

d) eine unabhängige Gewähr oder einen Auditbericht in Bezug auf das zuverlässige Management von Risiken vorlegen, die mit der Durchführung von TLPT verbunden sind, darunter auch der angemessene Schutz vertraulicher Informationen des Finanzunternehmens und ein Ausgleich der geschäftlichen Risiken des Finanzunternehmens;

e) ordnungsgemäß und vollständig durch einschlägige Berufshaftpflichtversicherungen abgesichert sind, einschließlich einer Versicherung gegen das Risiko von Fehlverhalten und Fahrlässigkeit.

(2) Beim Einsatz interner Tester gewährleisten Finanzunternehmen, dass neben den Anforderungen in Absatz 1 auch folgende Bedingungen erfüllt sind:

a) der Einsatz wurde von der jeweils zuständigen Behörde oder von der gemäß Artikel 26 Absätze 9 und 10 benannten einzigen staatlichen Behörde genehmigt;

b) die jeweils zuständige Behörde hat überprüft, dass das Finanzunternehmen über ausreichende Ressourcen verfügt und sichergestellt hat, dass während der Konzeptions- und Durchführungsphase der Tests keine Interessenkonflikte entstehen; und

c) der Anbieter von Bedrohungsanalysen gehört nicht dem Finanzunternehmen an.

(3) Finanzunternehmen stellen sicher, dass in Verträgen, die mit externen Testern geschlossen werden, eine ordentliche Handhabung der Ergebnisse von TLPT vorgesehen ist und die diesbezügliche Datenverarbeitung, einschließlich Generierung, Speicherung, Aggregation, Entwurf, Berichterstattung, Weitergabe oder Vernichtung, keine Risiken für das Finanzunternehmen mit sich bringt.

*KAPITEL V*

***Management des IKT-Drittparteienrisikos***

Abschnitt I

**Schlüsselprinzipien für ein solides Management des IKT-Drittparteienrisikos**

*Artikel 28*

**Allgemeine Prinzipien**

(1) Finanzunternehmen managen das IKT-Drittparteienrisiko als integralen Bestandteil des IKT-Risikos innerhalb ihres IKT-Risikomanagementrahmens nach Artikel 6 Absatz 1 und im Einklang mit den folgenden Prinzipien:

a) Finanzunternehmen, die vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen für die Ausübung ihrer Geschäftstätigkeit getroffen haben, bleiben jederzeit in vollem Umfang für die Einhaltung und Erfüllung aller Verpflichtungen nach dieser Verordnung und nach dem anwendbaren Finanzdienstleistungsrecht verantwortlich.

b) Beim Management des IKT-Drittparteienrisikos tragen Finanzunternehmen dem Grundsatz der Verhältnismäßigkeit Rechnung, wobei Folgendes zu berücksichtigen ist:

i) die Art, das Ausmaß, die Komplexität und die Relevanz IKT-bezogener Abhängigkeiten,

ii) die Risiken infolge vertraglicher Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen wurden, wobei die Kritikalität oder Relevanz der jeweiligen Dienstleistungen, Prozesse oder Funktionen sowie die potenziellen Auswirkungen auf die Kontinuität und Verfügbarkeit von Finanzdienstleistungen und -tätigkeiten auf Einzel- und Gruppenebene zu berücksichtigen sind.

(2) Finanzinstitute, bei denen es sich weder um die in Artikel 16 Absatz 1 Unterabsatz 1 genannten Unternehmen noch um Kleinstunternehmen handelt, beschließen im Rahmen ihres IKT-Risikomanagementrahmens eine Strategie für das IKT-Drittparteienrisiko und überprüfen diese regelmäßig, wobei gegebenenfalls die in Artikel 6 Absatz 9 genannte Strategie zur Nutzung mehrerer Anbieter Berücksichtigung findet. Die Strategie zum IKT-Drittparteienrisiko umfasst eine Leitlinie für die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, und gilt auf individueller und gegebenenfalls teilkonsolidierter und konsolidierter Basis. Das Leitungsorgan überprüft auf der Grundlage einer Bewertung des Gesamtrisikoprofils des Finanzunternehmens und des Umfangs und der Komplexität der Unternehmensdienstleistungen regelmäßig Risiken, die im Zusammenhang mit den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen ermittelt werden.

(3) Finanzunternehmen führen und aktualisieren im Rahmen ihres IKT-Risikomanagementrahmens auf Unternehmensebene sowie auf teilkonsolidierter und konsolidierter Ebene ein Informationsregister, das sich auf alle vertraglichen Vereinbarungen über die Nutzung von durch IKT-Drittdienstleister bereitgestellten IKT-Dienstleistungen bezieht.

Die vertraglichen Vereinbarungen gemäß Unterabsatz 1 werden angemessen dokumentiert, wobei zwischen Vereinbarungen, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen abdecken, und solchen unterschieden wird, bei denen dies nicht der Fall ist.

Finanzunternehmen erstatten den zuständigen Behörden mindestens einmal jährlich Bericht zur Anzahl neuer Vereinbarungen über die Nutzung von IKT-Dienstleistungen, den Kategorien von IKT-Drittdienstleistern, der Art der vertraglichen Vereinbarungen sowie den bereitgestellten IKT-Dienstleistungen und -Funktionen.

Finanzunternehmen stellen der zuständigen Behörde auf Verlangen das vollständige Informationsregister oder auf Anfrage bestimmte Teile dieses Registers zusammen mit allen Informationen zur Verfügung, die für eine wirksame Beaufsichtigung des Finanzunternehmens als notwendig erachtet werden.

Finanzunternehmen unterrichten die zuständige Behörde zeitnah über jede geplante vertragliche Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen sowie in dem Fall, dass eine Funktion kritisch oder wichtig geworden ist.

(4) Vor Abschluss einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen müssen Finanzunternehmen:

a) beurteilen, ob sich die vertragliche Vereinbarung auf die Nutzung von IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion bezieht;

b) beurteilen, ob die aufsichtsrechtlichen Bedingungen für die Auftragsvergabe erfüllt sind;

c) alle relevanten Risiken im Zusammenhang mit der vertraglichen Vereinbarung ermitteln und bewerten, einschließlich der Möglichkeit, dass diese vertragliche Vereinbarung dazu beitragen kann, das in Artikel 29 genannte IKT-Konzentrationsrisiko zu erhöhen;

d) bei potenziellen IKT-Drittdienstleistern der gebotenen Sorgfaltspflicht nachkommen und während des gesamten Auswahl- und Bewertungsprozesses sicherstellen, dass der IKT-Drittdienstleister geeignet ist;

e) Interessenkonflikte, die durch die vertragliche Vereinbarung entstehen können, ermitteln und bewerten.

(5) Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die angemessene Standards für Informationssicherheit einhalten. Betreffen diese vertraglichen Vereinbarungen kritische oder wichtige Funktionen, so berücksichtigen die Finanzunternehmen vor Abschluss der Vereinbarungen angemessen, ob die IKT-Drittdienstleister die aktuellsten und höchsten Qualitätsstandards für die Informationssicherheit anwenden.

(6) Bei der Ausübung der Zugangs-, Inspektions- und Auditrechte in Bezug auf den IKT-Drittdienstleister bestimmen Finanzunternehmen auf der Grundlage eines risikobasierten Ansatzes vorab die Häufigkeit von Audits und Inspektionen sowie die zu prüfenden Bereiche, indem allgemein anerkannte Auditstandards im Einklang mit etwaigen Aufsichtsanweisungen für die Anwendung und Einbeziehung solcher Auditstandards eingehalten werden.

Wenn vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen, die mit IKT-Drittdienstleistern geschlossen werden, ein hohes Maß an technischer Komplexität mit sich bringen, überprüft das Finanzunternehmen, dass die internen oder externen Revisoren oder ein Revisorenpool über die Fähigkeiten und Kenntnisse verfügen bzw. verfügt, die für die wirksame Durchführung der einschlägigen Audits und Bewertungen erforderlich sind.

(7) Finanzunternehmen stellen sicher, dass vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen gekündigt werden können, wenn einer der folgenden Umstände vorliegt:

a) ein erheblicher Verstoß des IKT-Drittdienstleisters gegen geltende Gesetze, sonstige Vorschriften oder Vertragsbedingungen;

b) Umstände, die im Laufe der Überwachung des IKT-Drittparteienrisikos festgestellt wurden und die als geeignet eingeschätzt werden, die Wahrnehmung der im Rahmen der vertraglichen Vereinbarung vorgesehenen Funktionen zu beeinträchtigen, einschließlich wesentlicher Änderungen, die sich auf die Vereinbarung oder die Verhältnisse des IKT-Drittdienstleisters auswirken;

c) nachweisliche Schwächen des IKT-Drittdienstleisters in Bezug auf sein allgemeines IKT-Risikomanagement und insbesondere bei der Art und Weise, in der er die Verfügbarkeit, Authentizität, Sicherheit und Vertraulichkeit von Daten gewährleistet, unabhängig davon, ob es sich um personenbezogene oder anderweitig sensible Daten oder nicht personenbezogene Daten handelt;

d) die zuständige Behörde kann das Finanzunternehmen infolge der Bedingungen der jeweiligen vertraglichen Vereinbarung oder der mit dieser Vereinbarung verbundenen Umstände nicht mehr wirksam beaufsichtigen.

(8) Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein. In den Ausstiegsstrategien wird den Risiken Rechnung getragen, die auf der Ebene der IKT-Drittdienstleister entstehen können, darunter insbesondere ein möglicher Fehler des IKT-Drittdienstleisters, eine Verschlechterung der Qualität der bereitgestellten IKT-Dienstleistungen, jede Unterbrechung der Geschäftstätigkeit aufgrund unangemessener oder unterlassener Bereitstellung von IKT-Dienstleistungen oder jedes erhebliche Risiko im Zusammenhang mit der angemessenen und kontinuierlichen Bereitstellung der jeweiligen IKT-Dienstleistungen oder der Beendigung vertraglicher Vereinbarungen mit IKT-Drittdienstleistern unter einem der in Absatz 7 genannten Umstände.

Finanzunternehmen stellen sicher, dass sie aus vertraglichen Vereinbarungen ausscheiden können, ohne:

a) Unterbrechung ihrer Geschäftstätigkeit,

b) Einschränkung der Einhaltung regulatorischer Anforderungen,

c) Beeinträchtigung der Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen.

Ausstiegspläne müssen umfassend, dokumentiert und im Einklang mit den in Artikel 4 Absatz 2 aufgeführten Kriterien ausreichend getestet sein sowie regelmäßig überprüft werden.

Finanzunternehmen ermitteln alternative Lösungen und entwickeln Übergangspläne, die es ihnen ermöglichen, dem IKT-Drittdienstleister die vertraglich vereinbarten IKT-Dienstleistungen und die relevanten Daten zu entziehen und sie sicher und vollständig alternativen Anbietern zu übertragen oder wieder in die eigenen Systeme zu überführen.

Finanzunternehmen verfügen über angemessene Notfallmaßnahmen, um die Fortführung der Geschäftstätigkeit zu gewährleisten, falls die in Unterabsatz 1 genannten Umstände auftreten.

(9) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Durchführungsstandards, um die Standardvorlagen für die Zwecke des in Absatz 3 genannten Informationsregisters festzulegen, einschließlich Informationen, die allen vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen gemein sind. Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die in Unterabsatz 1 genannten technischen Durchführungsstandards gemäß Artikel 15 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu erlassen.

(10) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe für technische Regulierungsstandards, um den detaillierten Inhalt der Leitlinie, die in Absatz 2 in Bezug auf die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer und wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, genannt wird, weiter zu spezifizieren.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte. Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Januar 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

*Artikel 29*

**Vorläufige Bewertung des IKT-Konzentrationsrisikos auf Unternehmensebene**

(1) Bei der Ermittlung und Bewertung der in Artikel 28 Absatz 4 Buchstabe c genannten Risiken berücksichtigen Finanzunternehmen zudem, ob der geplante Abschluss einer vertraglichen Vereinbarung in Bezug auf IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, Folgendes herbeiführen würde:

a) Verträge mit einem IKT-Drittdienstleister, der nicht ohne Weiteres ersetzbar ist; oder

b) mehrfache vertragliche Vereinbarungen über die Bereitstellung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen mit demselben IKT-Drittdienstleister oder mit eng verbundenen IKT-Drittdienstleistern.

Finanzunternehmen wägen Nutzen und Kosten alternativer Lösungen ab, z. B. die Nutzung verschiedener IKT-Drittdienstleister, und berücksichtigen, ob und wie geplante Lösungen den geschäftlichen Erfordernissen und Zielen entsprechen, die in ihrer Strategie für digitale Resilienz festgelegt sind.

(2) Ist in der vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Möglichkeit vorgesehen, dass ein IKT-Drittdienstleister IKT-Dienstleistungen zur Unterstützung einer kritischen oder wichtigen Funktion per Unterauftrag an andere IKT-Drittdienstleister vergibt, wägen Finanzunternehmen die Vorteile und Risiken ab, die im Zusammenhang mit einer solchen Unterauftragsvergabe entstehen können, insbesondere sofern der IKT-Unterauftragnehmer in einem Drittland niedergelassen ist.

Betreffen vertragliche Vereinbarungen IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, berücksichtigen die Finanzunternehmen gebührend die Bestimmungen des Insolvenzrechts, die im Falle der Insolvenz des IKT-Drittdienstleisters anwendbar wären, sowie jede Einschränkung, die sich im Zusammenhang mit der dringenden Wiederherstellung der Daten des Finanzunternehmens ergeben könnte.

Werden mit einem IKT-Drittdienstleister mit Sitz in einem Drittland vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen geschlossen, so beachten Finanzunternehmen neben den in Unterabsatz 2 genannten Umständen auch, dass die Datenschutzvorschriften der Union eingehalten und die Rechtsvorschriften in diesem Drittland wirksam durchgesetzt werden.

Ist in den vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen die Unterauftragsvergabe vorgesehen, so bewerten die Finanzunternehmen, ob und wie sich potenziell lange oder komplexe Ketten der Unterauftragsvergabe auf ihre Fähigkeit auswirken können, die vertraglich vereinbarten Funktionen vollständig zu überwachen, und ob die zuständige Behörde in dieser Hinsicht in der Lage ist, das Finanzunternehmen wirksam zu beaufsichtigen.

*Artikel 30*

**Wesentliche Vertragsbestimmungen**

(1) Die Rechte und Pflichten des Finanzunternehmens und des IKT-Drittdienstleisters werden eindeutig zugewiesen und schriftlich dargelegt. Der vollständige Vertrag umfasst die Vereinbarung über die Dienstleistungsgüte und wird in einem schriftlichen Dokument, das den Parteien in Papierform zur Verfügung steht, oder in einem Dokument in einem anderen herunterladbaren, dauerhaften und zugänglichen Format dokumentiert.

(2) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfassen mindestens folgende Elemente:

a) eine klare und vollständige Beschreibung aller Funktionen und IKT-Dienstleistungen, die der IKT-Drittdienstleister bereitzustellen hat, wobei anzugeben ist, ob die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist, und — wenn dies der Fall ist — welche Bedingungen für diese Unterauftragsvergabe gelten;

b) die Standorte — das heißt die Regionen oder Länder —, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind und an denen Daten verarbeitet werden sollen, einschließlich des Speicherorts, sowie die Auflage für den IKT-Drittdienstleister, das Finanzunternehmen vorab zu benachrichtigen, wenn er eine Änderung dieser Standorte beabsichtigt;

c) Bestimmungen über Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit in Bezug auf den Datenschutz, einschließlich des Schutzes personenbezogener Daten;

d) Bestimmungen über die Sicherstellung des Zugangs zu personenbezogenen und nicht personenbezogenen Daten, die von dem Finanzunternehmen im Fall einer Insolvenz, Abwicklung, Einstellung der Geschäftstätigkeit des IKT-Drittdienstleisters oder einer Beendigung der vertraglichen Vereinbarungen verarbeitet werden, sowie über die Wiederherstellung und Rückgabe dieser Daten in einem leicht zugänglichen Format;

e) Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen;

f) die Verpflichtung des IKT-Drittdienstleisters, dem Finanzunternehmen bei einem IKT-Vorfall, der mit dem für das Finanzunternehmen bereitgestellten IKT-Dienst in Verbindung steht, ohne zusätzliche Kosten oder zu vorab festzusetzenden Kosten Unterstützung zu leisten;

g) die Verpflichtung des IKT-Drittdienstleisters, vollumfänglich mit den für das Finanzunternehmen zuständigen Behörden und Abwicklungsbehörden zusammenzuarbeiten, einschließlich der von diesen benannten Personen;

h) Kündigungsrechte und damit zusammenhängende Mindestkündigungsfristen für die Beendigung der vertraglichen Vereinbarungen entsprechend den Erwartungen der zuständigen Behörden und der Abwicklungsbehörden;

i) Bedingungen für die Teilnahme von IKT-Drittdienstleistern an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz gemäß Artikel 13 Absatz 6.

(3) Die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen umfassen zusätzlich zu den in Absatz 2 genannten Elementen mindestens Folgendes:

a) vollständige Beschreibungen der Dienstleistungsgüte, einschließlich Aktualisierungen und Überarbeitungen, mit präzisen quantitativen und qualitativen Leistungszielen innerhalb der vereinbarten Dienstleistungsgüte, um dem Finanzunternehmen eine wirksame Überwachung von IKT-Dienstleistungen und das unverzügliche Ergreifen angemessener Korrekturmaßnahmen zu ermöglichen, wenn eine vereinbarte Dienstleistungsgüte nicht erreicht wird;

b) Kündigungsfristen und Berichtspflichten des IKT-Drittdienstleisters gegenüber dem Finanzunternehmen, einschließlich der Meldung aller Entwicklungen, die sich wesentlich auf die Fähigkeit des IKT-Drittdienstleisters, IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen gemäß den vereinbarten Leistungsniveaus wirksam bereitzustellen, auswirken könnten;

c) Anforderungen an den IKT-Drittdienstleister, Notfallpläne zu implementieren und zu testen und über Maßnahmen, Tools und Leit- und Richtlinien für IKT-Sicherheit zu verfügen, die ein angemessenes Maß an Sicherheit für die Erbringung von Dienstleistungen durch das Finanzunternehmen im Einklang mit seinem Rechtsrahmen bieten;

d) die Verpflichtung des IKT-Drittdienstleisters, sich an den in den Artikeln 26 und 27 genannten TLPT des Finanzunternehmens zu beteiligen und uneingeschränkt daran mitzuwirken;

e) das Recht, die Leistung des IKT-Drittdienstleisters fortlaufend zu überwachen, wozu Folgendes gehört:

i) uneingeschränkte Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens oder eines beauftragten Dritten und der zuständigen Behörde sowie das Recht auf Anfertigung von Kopien einschlägiger Unterlagen vor Ort, wenn ihnen für die Geschäftstätigkeit des IKT-Drittdienstleisters entscheidende Bedeutung zukommt, wobei die tatsächliche Ausübung dieser Rechte nicht durch andere vertragliche Vereinbarungen oder Umsetzungsrichtlinien behindert oder eingeschränkt wird;

ii) das Recht, alternative Bestätigungsniveaus zu vereinbaren, wenn die Rechte anderer Kunden betroffen sind;

iii) die Verpflichtung des IKT-Drittdienstleisters zur uneingeschränkten Zusammenarbeit bei Vor-Ort-Inspektionen und Audits, die von den zuständigen Behörden, der federführenden Überwachungsbehörde, dem Finanzunternehmen oder einem beauftragten Dritten durchgeführt werden; und

iv) die Verpflichtung, Einzelheiten zu Umfang und Häufigkeit dieser Inspektionen sowie dem dabei zu befolgenden Verfahren mitzuteilen;

f) Ausstiegsstrategien, insbesondere die Festlegung eines verbindlichen angemessenen Übergangszeitraums,

i) in dem der IKT-Drittdienstleister weiterhin die entsprechenden Funktionen oder IKT-Dienstleistungen bereitstellt, um das Risiko von Störungen im Finanzunternehmen zu verringern oder um dessen geordnete Abwicklung und Umstrukturierung sicherzustellen;

ii) der dem Finanzunternehmen ermöglicht, zu einem anderen IKT-Drittdienstleister zu wechseln oder auf interne Lösungen umzustellen, die der Komplexität der erbrachten Dienstleistung entsprechen.

Abweichend von Buchstabe e können der IKT-Drittdienstleister und das Finanzunternehmen, das ein Kleinstunternehmen ist, vereinbaren, dass die Zugangs-, Inspektions- und Auditrechte des Finanzunternehmens auf einen unabhängigen Dritten übertragen werden können, der vom IKT-Drittdienstleister benannt wird, sowie dass das Finanzunternehmen von diesem Dritten jederzeit Informationen und Gewähr in Bezug auf die Leistung des IKT-Drittdienstleisters verlangen kann.

(4) Bei der Aushandlung vertraglicher Vereinbarungen erwägen Finanzunternehmen und IKT-Drittdienstleister die Verwendung von Standardvertragsklauseln, die von Behörden für bestimmte Dienstleistungen entwickelt wurden.

(5) Die ESA erarbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards, um die in Absatz 2 Buchstabe a genannten Aspekte zu präzisieren, die ein Finanzunternehmen bei der Untervergabe von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen bestimmen und bewerten muss.

Bei der Ausarbeitung dieser Entwürfe technischer Regulierungsstandards berücksichtigen die ESA die Größe und das Gesamtrisikoprofil des Finanzunternehmens sowie die Art, den Umfang und die Komplexität seiner Dienstleistungen, Tätigkeiten und Geschäfte.

Die ESA übermitteln der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme der in Unterabsatz 1 genannten technischen Regulierungsstandards gemäß den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

## Abschnitt II

## **Überwachungsrahmen für kritische IKT-Drittdienstleister**

### *Artikel 31*

### **Einstufung kritischer IKT-Drittdienstleister**

(1) Die ESA nehmen über den Gemeinsamen Ausschuss und auf Empfehlung des gemäß Artikel 32 Absatz 1 eingerichteten Überwachungsforums folgende Aufgaben wahr:

a) Einstufung der IKT-Drittdienstleister, die für Finanzunternehmen kritisch sind, nachdem eine entsprechende Bewertung unter Berücksichtigung der in Absatz 2 genannten Kriterien durchgeführt wurde;

b) Ernennung derjenigen Europäischen Aufsichtsbehörde zur federführenden Überwachungsbehörde für jeden kritischen IKT-Drittdienstleister, die gemäß den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 bzw. (EU) Nr. 1095/2010 für diejenigen Finanzunternehmen zuständig ist, die nachweislich der Summe der einzelnen Bilanzen dieser Finanzunternehmen zusammen den größten Anteil des Gesamtvermögens am Gesamtwert der Aktiva aller Finanzunternehmen halten, die die Dienste des betreffenden kritischen IKT-Drittdienstleisters nutzen.

(2) Die Einstufung nach Absatz 1 Buchstabe a basiert in Bezug auf IKT-Dienstleistungen, die vom IKT-Drittdienstleister bereitgestellt werden, auf den folgenden Kriterien:

a) den systemischen Auswirkungen auf die Stabilität, Kontinuität oder Qualität der Erbringung von Finanzdienstleistungen, falls der betreffende IKT-Drittdienstleister bei der Erbringung seiner Dienste einer umfassenden Betriebsstörung ausgesetzt wäre, wobei die Zahl von Finanzunternehmen und der Gesamtwert der Aktiva derjenigen Finanzunternehmen zu berücksichtigen ist, für die der betreffende IKT-Drittdienstleister Dienstleistungen erbringt;

b) dem systemischen Charakter oder der Bedeutung der Finanzunternehmen, die auf den jeweiligen IKT-Drittdienstleister zurückgreifen, bewertet anhand der folgenden Parameter:

   i) der Anzahl global systemrelevanter Institute (G-SRI) oder anderer systemrelevanter Institute (A-SRI), die auf den jeweiligen IKT-Drittdienstleister zurückgreifen;

   ii) der Interdependenz zwischen den unter Ziffer i genannten G-SRI oder A-SRI und anderen Finanzunternehmen, einschließlich der Fälle, in denen die G-SRI oder A-SRI Finanzinfrastrukturdienstleistungen für andere Finanzunternehmen erbringen;

c) der Abhängigkeit von Finanzunternehmen von den Dienstleistungen des betreffenden IKT-Drittdienstleisters mit Blick auf kritische oder wichtige Funktionen von Finanzunternehmen, in die letztlich derselbe IKT-Drittdienstleister involviert ist — unabhängig davon, ob Finanzunternehmen diese Dienste direkt oder indirekt durch Vereinbarungen über die Unterauftragsvergabe in Anspruch nehmen;

d) dem Grad der Substituierbarkeit des IKT-Drittdienstleisters unter Berücksichtigung der folgenden Parameter:

   i) des Mangels an echten, auch teilweisen Alternativen aufgrund der begrenzten Zahl von IKT-Drittdienstleistern, die auf einem bestimmten Markt tätig sind, oder des Marktanteils des betreffenden IKT-Drittdienstleisters oder der damit verbundenen technischen Komplexität oder Differenziertheit, auch in Bezug auf proprietäre Technologien, oder der besonderen Merkmale der Organisation oder Tätigkeit des IKT-Drittdienstleisters;

   ii) der Schwierigkeiten bei der teilweisen oder vollständigen Migration der einschlägigen Daten und Arbeitslasten vom jeweiligen IKT-Drittdienstleister zu einem anderen IKT-Drittdienstleister, die entweder auf erhebliche finanzielle Kosten, zeitliche oder sonstige Ressourcen, die der Migrationsprozess mit sich bringen kann, oder auf erhöhte IKT-Risiken oder sonstige operationelle Risiken zurückzuführen sind, denen das Finanzunternehmen durch eine solche Migration ausgesetzt sein könnte.

(3) Gehört der IKT-Drittdienstleister zu einer Gruppe, so werden die in Absatz 2 genannten Kriterien in Bezug auf die von der Gruppe als Ganzes bereitgestellten IKT-Dienstleistungen berücksichtigt.

(4) Kritische IKT-Drittdienstleister, die Teil einer Gruppe sind, benennen eine juristische Person als Koordinierungsstelle, um eine angemessene Vertretung und Kommunikation mit der federführenden Überwachungsbehörde sicherzustellen.

(5) Die federführende Überwachungsbehörde unterrichtet den IKT-Drittdienstleister über das Ergebnis der Bewertung, die zu der in Absatz 1 Buchstabe a genannten Einstufung geführt hat. Innerhalb von sechs Wochen ab dem Datum der Unterrichtung kann der IKT-Drittdienstleister der federführenden Überwachungsbehörde eine begründete Erklärung mit allen für die Zwecke der Bewertung relevanten Informationen übermitteln. Die federführende Überwachungsbehörde prüft die begründete Erklärung und kann verlangen, dass innerhalb von 30 Kalendertagen nach Eingang der Erklärung zusätzliche Informationen übermittelt werden.

Nach der Einstufung eines IKT-Drittdienstleisters als kritisch, unterrichten die ESA den IKT-Drittdienstleister über den Gemeinsamen Ausschuss über diese Einstufung und das Anfangsdatum, ab dem er tatsächlich Überwachungstätigkeiten unterliegen wird. Dieses Anfangsdatum darf nicht mehr als einen Monat nach der Unterrichtung liegen. Der IKT-Drittdienstleister teilt den Finanzunternehmen, für die er Dienstleistungen erbringt, seine Einstufung als kritisch mit.

(6) Der Kommission wird die Befugnis übertragen, gemäß Artikel 57 einen delegierten Rechtsakt zu erlassen, um diese Verordnung durch die weitere Präzisierung der in Absatz 2 genannten Kriterien bis 17. Juli 2024 zu ergänzen.

(7) Die Einstufung nach Absatz 1 Buchstabe a darf erst angewendet werden, wenn die Kommission einen delegierten Rechtsakt gemäß Absatz 6 erlassen hat.

(8) Die Einstufung nach Absatz 1 Buchstabe a gilt nicht für:

i) Finanzunternehmen, die IKT-Dienstleistungen für andere Finanzunternehmen bereitstellen;

ii) IKT-Drittdienstleister, die Überwachungsrahmen unterliegen, die zur Unterstützung der in Artikel 127 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union genannten Aufgaben eingerichtet wurden;

iii) gruppeninterne IKT-Dienstleister;

iv) IKT-Drittdienstleister, die IKT-Dienstleistungen ausschließlich in einem Mitgliedstaat für Finanzunternehmen bereitstellen, die nur in diesem Mitgliedstaat tätig sind.

(9) Die ESA erstellen, veröffentlichen und aktualisieren die Liste kritischer IKT-Drittdienstleister auf Unionsebene jährlich über den Gemeinsamen Ausschuss.

(10) Die zuständigen Behörden übermitteln dem gemäß Artikel 32 eingerichteten Überwachungsforum für die Zwecke von Absatz 1 Buchstabe a die in Artikel 28 Absatz 3 Unterabsatz 3 genannten Berichte auf jährlicher und aggregierter Basis. Das Überwachungsforum bewertet die Abhängigkeiten von Finanzunternehmen gegenüber IKT-Drittdienstleistern auf der Grundlage der von den zuständigen Behörden übermittelten Informationen.

(11) Diejenigen IKT-Drittdienstleister, die nicht in der in Absatz 9 genannten Liste aufgeführt sind, können beantragen, gemäß Absatz 1 Buchstabe a als kritisch eingestuft zu werden.

Für die Zwecke von Unterabsatz 1 reicht der IKT-Drittdienstleister bei der EBA, der ESMA oder der EIOPA einen begründeten Antrag ein, die über den Gemeinsamen Ausschuss entscheiden, ob dieser IKT-Drittdienstleister gemäß Absatz 1 Buchstabe a als kritisch eingestuft werden soll.

Die in Unterabsatz 2 genannte Entscheidung wird innerhalb von 6 Monaten nach Eingang des Antrags getroffen und dem IKT-Drittdienstleister mitgeteilt.

(12) Finanzunternehmen dürfen nur dann die Dienstleistungen eines IKT-Drittdienstleisters mit Sitz in einem Drittland in Anspruch nehmen, der gemäß Absatz 1 Buchstabe a als kritisch eingestuft worden ist, wenn er innerhalb von zwölf Monaten nach der Einstufung ein Tochterunternehmen in der Union gegründet hat.

(13) Der in Absatz 12 genannte kritische IKT-Drittdienstleister teilt der federführenden Überwachungsbehörde jede Änderung der Leitungsstruktur des in der Union niedergelassenen Tochterunternehmens mit.

*Artikel 32*

**Struktur des Überwachungsrahmens**

(1) Der Gemeinsame Ausschuss richtet gemäß Artikel 57 Absatz 1 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 das Überwachungsforum als Unterausschuss ein, der die Arbeit des Gemeinsamen Ausschusses und der in Artikel 31 Absatz 1 Buchstabe b genannten federführenden Überwachungsbehörde im Bereich des IKT-Drittparteienrisikos in allen Finanzsektoren unterstützt. Das Überwachungsforum erarbeitet die Entwürfe gemeinsamer Positionen und gemeinsamer Maßnahmen des Gemeinsamen Ausschusses in diesem Bereich.

Das Überwachungsforum erörtert regelmäßig einschlägige Entwicklungen in Bezug auf IKT-Risiken und -Schwachstellen und fördert einen kohärenten Ansatz bei der Überwachung des IKT-Drittparteienrisikos auf Unionsebene.

(2) Das Überwachungsforum führt jährlich eine gemeinsame Bewertung der Ergebnisse und Erkenntnisse der Überwachungstätigkeiten durch, die für alle kritischen IKT-Drittdienstleister durchgeführt wurden, und fördert Koordinierungsmaßnahmen, um die digitale operationale Resilienz von Finanzunternehmen zu erhöhen, bewährte Verfahren zum Angehen des IKT-Konzentrationsrisikos zu fördern und Möglichkeiten zur Abschwächung sektorübergreifender Risikotransfers zu untersuchen.

(3) Das Überwachungsforum legt umfassende Referenzwerte für kritische IKT-Drittdienstleister vor, die vom Gemeinsamen Ausschuss als gemeinsame Positionen der ESA gemäß Artikel 56 Absatz 1 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 anzunehmen sind.

(4) Das Überwachungsforum setzt sich zusammen aus

a) den Vorsitzenden der ESA;

b) einem hochrangigen Vertreter des aktuellen Personals der in Artikel 46 genannten betreffenden zuständigen Behörde eines jeden Mitgliedstaats;

c) den Exekutivdirektoren jeder Europäischen Aufsichtsbehörde und einem Vertreter der Kommission, des ESRB, der EZB und der ENISA als Beobachter;

d) gegebenenfalls einem zusätzlichen Vertreter einer in Artikel 46 genannten zuständigen Behörde eines jeden Mitgliedstaats als Beobachter;

e) gegebenenfalls einem Vertreter der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden, der für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig ist, als Beobachter.

Das Überwachungsforum kann gegebenenfalls den Rat unabhängiger Sachverständiger einholen, die gemäß Absatz 6 ernannt wurden.

(5) Jeder Mitgliedstaat benennt die jeweils zuständige Behörde, deren Mitarbeiter der in Absatz 4 Unterabsatz 1 Buchstabe b genannte hochrangige Vertreter ist, und setzt die federführende Überwachungsbehörde davon in Kenntnis.

Die ESA veröffentlichen auf ihrer Website die Liste der von den Mitgliedstaaten benannten hochrangigen Vertreter aus dem aktuellen Personal der jeweils zuständigen Behörde.

(6) Die in Absatz 4 Unterabsatz 2 genannten unabhängigen Sachverständigen werden vom Überwachungsforum aus einem Pool von Sachverständigen ernannt, die im Anschluss an ein öffentliches und transparentes Bewerbungsverfahren ausgewählt wurden.

Die unabhängigen Sachverständigen werden auf der Grundlage ihres Fachwissens in den Bereichen Finanzstabilität, digitale operationale Resilienz und Fragen der IKT-Sicherheit ernannt. Sie handeln unabhängig und objektiv im alleinigen Interesse der Union als Ganzes und dürfen von Organen oder Einrichtungen der Union, von der Regierung eines Mitgliedstaats oder von öffentlichen oder privaten Stellen Weisungen weder einholen noch entgegennehmen.

(7) Gemäß Artikel 16 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 geben die ESA für die Zwecke dieses Abschnitts bis zum 17. Juli 2024 Leitlinien für die Zusammenarbeit zwischen den ESA und den zuständigen Behörden heraus, die die detaillierten Verfahren und Bedingungen für die Zuweisung und Ausführung von Aufgaben zwischen zuständigen Behörden und den ESA sowie die Einzelheiten zum Austausch von Informationen regeln, die zuständige Behörden benötigen, um die Weiterbehandlung der in Artikel 35 Absatz 1 Buchstabe d genannten Empfehlungen zu gewährleisten, die an kritische IKT-Drittdienstleister gerichtet werden.

(8) Die in diesem Abschnitt dargelegten Anforderungen gelten unbeschadet der Anwendung der Richtlinie (EU) 2022/2555 und anderer Überwachungsvorschriften der Union, die für Anbieter von Cloud-Computing-Diensten gelten.

(9) Die ESA legen dem Europäischen Parlament, dem Rat und der Kommission über den Gemeinsamen Ausschuss und auf der Grundlage von Vorarbeiten des Überwachungsforums jährlich einen Bericht über die Anwendung dieses Abschnitts vor.

*Artikel 33*

**Aufgaben der federführenden Überwachungsbehörde**

(1) Die gemäß Artikel 31 Absatz 1 Buchstabe b ernannte federführende Überwachungsbehörde führt die Überwachung über die zugewiesenen kritischen IKT-Drittdienstleister durch und ist für diese kritischen IKT-Drittdienstleister für die Zwecke aller mit der Überwachung verbundenen Angelegenheiten die vorrangige Anlaufstelle.

(2) Für die Zwecke des Absatzes 1 bewertet die federführende Überwachungsbehörde, ob jeder kritische IKT-Drittdienstleister über umfassende, fundierte und wirksame Vorschriften, Verfahren, Mechanismen und Vorkehrungen für das Management der IKT-Risiken verfügt, die er für Finanzunternehmen mit sich bringen kann.

Bei der in Unterabsatz 1 genannten Bewertung stehen vor allem IKT-Dienstleistungen im Mittelpunkt, die von dem kritischen IKT-Drittdienstleister bereitgestellt werden und kritische oder wichtige Funktionen von Finanzunternehmen unterstützen. Diese Bewertung wird auf IKT-Dienstleistungen, die andere als kritische oder wichtige Funktionen unterstützen, ausgeweitet, wenn dies zur Bewältigung aller relevanten Risiken erforderlich ist.

(3) Die in Absatz 2 genannte Bewertung erstreckt sich auf

a) IKT-Anforderungen, um insbesondere die Sicherheit, Verfügbarkeit, Kontinuität, Skalierbarkeit und Qualität der Dienste zu gewährleisten, die der kritische IKT-Drittdienstleister für Finanzunternehmen erbringt, sowie die Fähigkeit, jederzeit hohe Standards in Bezug auf Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit der Daten aufrechtzuerhalten;

b) die physische Sicherheit, die zur Gewährleistung der IKT-Sicherheit beiträgt, darunter auch die Sicherheit von Räumlichkeiten, Einrichtungen und Datenzentren;

c) Risikomanagementprozesse, einschließlich Strategien für IKT-Risikomanagement, IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungsplänen;

d) Governance-Regelungen, einschließlich einer Organisationsstruktur mit klaren, transparenten und kohärenten Zuständigkeits- und Rechenschaftspflichten, die ein wirksames IKT-Risikomanagement ermöglichen;

e) die Ermittlung, Überwachung und unverzügliche Meldung wesentlicher IKT-bezogener Vorfälle an die Finanzunternehmen sowie den Umgang mit und die Lösung dieser Vorfälle, insbesondere Cyberangriffe;

f) Mechanismen für Datenübertragbarkeit, Übertragbarkeit von Anwendungen und Interoperabilität, die eine wirksame Wahrnehmung von Kündigungsrechten durch die Finanzunternehmen gewährleisten;

g) Tests von IKT-Systemen, Infrastrukturen und Kontrollen;

h) IKT-Audits;

i) die Übernahme einschlägiger nationaler und internationaler Normen, die auf die Erbringung der IKT-Dienstleistungen für Finanzunternehmen anwendbar sind.

(4) Die federführende Überwachungsbehörde nimmt auf der Grundlage der in Absatz 2 genannten Bewertung und in Abstimmung mit dem in Artikel 34 Absatz 1 genannten gemeinsamen Überwachungsnetz (Joint Oversight Network — JON) einen klaren, detaillierten und durchdachten individuellen Überwachungsplan an, in dem die für jeden kritischen IKT-Drittdienstleister vorgesehenen jährlichen Überwachungsziele und wichtigsten Überwachungsmaßnahmen beschrieben werden. Dieser Plan wird dem kritischen IKT-Drittdienstleister jedes Jahr übermittelt.

Vor der Annahme des Überwachungsplans übermittelt die federführende Überwachungsbehörde dem kritischen IKT-Drittdienstleister den Entwurf des Überwachungsplans.

Nach Eingang des Entwurfs des Überwachungsplans kann der kritische IKT-Drittdienstleister innerhalb von 15 Kalendertagen eine begründete Erklärung vorlegen, in der die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, aufgezeigt werden und gegebenenfalls Lösungen zur Risikominderung enthalten sind.

(5) Sobald die in Absatz 4 genannten jährlichen Überwachungspläne angenommen und den kritischen IKT-Drittdienstleistern übermittelt wurden, dürfen die zuständigen Behörden Maßnahmen in Bezug auf diese kritischen IKT-Drittdienstleister nur im Einvernehmen mit der federführenden Überwachungsbehörde ergreifen.

*Artikel 34*

**Operative Zusammenarbeit zwischen den federführenden Überwachungsbehörden**

(1) Um einen kohärenten Ansatz bei den Überwachungstätigkeiten sicherzustellen und um koordinierte allgemeine Überwachungsstrategien und kohärente operative Ansätze und Arbeitsmethoden sicherzustellen, richten die drei gemäß Artikel 31 Absatz 1 Buchstabe b benannten federführenden Überwachungsbehörden ein JON ein, um sich in den Vorbereitungsphasen untereinander abzustimmen und die Überwachung über die von ihnen jeweils überwachten kritischen IKT-Drittdienstleister sowie über das etwaige Vorgehen, das gemäß Artikel 42 erforderlich sein könnte, zu koordinieren.

(2) Für die Zwecke von Absatz 1 erstellen die federführenden Überwachungsbehörden ein gemeinsames Überwachungsprotokoll, in dem die genauen Verfahren für die tägliche Koordinierung und die Gewährleistung eines raschen Austauschs und rascher Reaktionen festgelegt sind. Das Protokoll wird regelmäßig überarbeitet, um den operativen Erfordernissen, insbesondere der Entwicklung praktischer Überwachungsregelungen, Rechnung zu tragen.

(3) Die federführenden Überwachungsbehörden können die EZB und die ENISA auf Ad-hoc-Basis ersuchen, fachliche Beratung zu leisten, praktische Erfahrungen auszutauschen oder an spezifischen Koordinierungssitzungen des JON teilzunehmen.

*Artikel 35*

**Befugnisse der federführenden Überwachungsbehörde**

(1) Die federführende Überwachungsbehörde hat zur Wahrnehmung der in diesem Abschnitt dargelegten Aufgaben in Bezug auf die kritischen IKT-Drittdienstleister die Befugnis,

a) alle einschlägigen Informationen und Unterlagen gemäß Artikel 37 anzufordern;

b) allgemeine Untersuchungen und Inspektionen gemäß den Artikeln 38 bzw. 39 durchzuführen;

c) nach Abschluss der Überwachungstätigkeiten Berichte anzufordern, in denen die ergriffenen Maßnahmen oder die Abhilfemaßnahmen aufgeführt sind, die von den kritischen IKT-Drittdienstleistern in Bezug auf die in Buchstabe d dieses Absatzes genannten Empfehlungen ergriffen wurden;

d) Empfehlungen zu den in Artikel 33 Absatz 3 genannten Bereichen abzugeben, insbesondere in Bezug auf Folgendes:

   i) die Anwendung spezifischer IKT-Sicherheits- und Qualitätsanforderungen oder -verfahren, insbesondere in Bezug auf die Herausgabe von Patches, Aktualisierungen, Verschlüsselung und andere Sicherheitsmaßnahmen, die die federführende Überwachungsbehörde für die Gewährleistung der IKT-Sicherheit von Diensten, die Finanzunternehmen bereitgestellt werden, für relevant hält;

   ii) die Verwendung von Bedingungen — einschließlich ihrer technischen Umsetzung — zu denen die kritischen IKT-Drittdienstleister IKT-Dienstleistungen für Finanzunternehmen bereitstellen, die die federführende Überwachungsbehörde für relevant hält, um die Entstehung punktueller Ausfälle oder deren Verstärkung zu verhindern oder um mögliche systemische Auswirkungen im Finanzsektor der Union im Falle eines IKT-Konzentrationsrisikos zu minimieren;

   iii) jede geplante Unterauftragsvergabe, in deren Fall die federführende Überwachungsbehörde aufgrund der Prüfung der gemäß den Artikeln 37 und 38 erlangten Informationen der Auffassung ist, dass eine weitere Unterauftragsvergabe, einschließlich Vereinbarungen über die Unterauftragsvergabe, die die kritischen IKT-Drittdienstleister mit anderen IKT-Drittdienstleistern oder mit IKT-Unterauftragnehmern mit Sitz in einem Drittland zu schließen beabsichtigen, Risiken für die Erbringung von Dienstleistungen durch das Finanzunternehmen oder Risiken für die Finanzstabilität mit sich bringen kann;

   iv) von der Vereinbarung über weitere Unterauftragsvergabe abzusehen, wenn die folgenden kumulativen Bedingungen erfüllt sind:

      — Bei dem ausgewählten Unterauftragnehmer handelt es sich um einen IKT-Drittdienstleister oder einen IKT-Unterauftragnehmer mit Sitz in einem Drittland;

      — die Unterauftragsvergabe betrifft eine kritische oder wichtige Funktion des Finanzunternehmens; und

— die federführende Überwachungsbehörde ist der Ansicht, dass diese Unterauftragsvergabe ein eindeutiges und ernstes Risiko für die Finanzstabilität der Union oder für Finanzunternehmen darstellt, einschließlich der Fähigkeit von Finanzunternehmen, Aufsichtsanforderungen zu erfüllen.

Für die Zwecke der Ziffer iv des vorliegenden Buchstabens übermitteln IKT-Drittdienstleister der federführenden Überwachungsbehörde unter Verwendung der in Artikel 41 Absatz 1 Buchstabe b genannten Vorlage Informationen über die Unterauftragsvergabe.

(2) Bei der Ausübung der in diesem Artikel genannten Befugnisse geht die federführende Überwachungsbehörde wie folgt vor:

a) Sie sorgt für eine regelmäßige Abstimmung innerhalb des JON und bemüht sich gegebenenfalls insbesondere um kohärente Herangehensweisen für die Überwachung kritischer IKT-Drittdienstleister;

b) sie trägt dem durch die Richtlinie (EU) 2022/2555 geschaffenen Rahmen gebührend Rechnung und konsultiert erforderlichenfalls die gemäß der genannten Richtlinie benannten oder eingerichteten zuständigen Behörden, um eine Überschneidung von technischen und organisatorischen Maßnahmen zu vermeiden, die gemäß der genannten Richtlinie auf kritische IKT-Drittdienstleister angewandt werden könnten;

c) sie ist bestrebt, das Risiko einer Störung der Dienste, die von kritischen IKT-Drittdienstleistern für Kunden bereitgestellt werden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, so weit wie möglich zu minimieren.

(3) Die federführende Überwachungsbehörde konsultiert das Überwachungsforum, bevor sie die in Absatz 1 genannten Befugnisse ausübt.

Bevor die federführende Überwachungsbehörde Empfehlungen gemäß Absatz 1 Buchstabe d abgibt, bietet die sie dem IKT-Drittdienstleister Gelegenheit, innerhalb von 30 Kalendertagen einschlägige Informationen bereitzustellen, mit denen die erwarteten Auswirkungen auf Kunden, bei denen es sich um nicht in den Anwendungsbereich dieser Verordnung fallende Unternehmen handelt, aufgezeigt werden und die gegebenenfalls Lösungen zur Risikominderung enthalten.

(4) Die federführende Überwachungsbehörde unterrichtet das JON über das Ergebnis der Ausübung der in Absatz 1 Buchstaben a und b genannten Befugnisse. Sie übermittelt die in Absatz 1 Buchstabe c genannten Berichte unverzüglich dem JON und den Behörden, die für diejenigen Finanzunternehmen, die die IKT-Dienstleistungen des betreffenden kritischen IKT-Drittdienstleisters in Anspruch nehmen, zuständig sind.

(5) Kritische IKT-Drittdienstleister arbeiten nach Treu und Glauben mit der federführenden Überwachungsbehörde zusammen und unterstützen sie bei der Erfüllung ihrer Aufgaben.

(6) Bei vollständiger oder teilweiser Nichteinhaltung der Maßnahmen, die infolge der Ausübung der Befugnisse gemäß Absatz 1 Buchstaben a, b oder c zu ergreifen sind, und nach Ablauf einer Frist von mindestens 30 Kalendertagen ab dem Tag, an dem der kritische IKT-Drittdienstleister eine Mitteilung über die betreffenden Maßnahmen erhalten hat, erlässt die federführende Überwachungsbehörde eine Entscheidung über die Verhängung eines Zwangsgelds, um den kritischen IKT-Drittdienstleister zur Einhaltung dieser Maßnahmen zu zwingen.

(7) Das in Absatz 6 genannte Zwangsgeld wird täglich bis zur Einhaltung der Vorschriften und für höchstens sechs Monate nach Mitteilung der Entscheidung über die Verhängung eines Zwangsgelds an den kritischen IKT-Drittdienstleister verhängt.

(8) Die Höhe des Zwangsgelds, berechnet ab dem in der Entscheidung über die Verhängung des Zwangsgelds genannten Zeitpunkt, beträgt bis zu 1 % des durchschnittlichen weltweiten Tagesumsatzes, den der kritische IKT-Drittdienstleister im vorangegangenen Geschäftsjahr erzielt hat. Bei der Festsetzung der Höhe des Zwangsgelds berücksichtigt die federführende Überwachungsbehörde in Bezug auf die Nichteinhaltung der in Absatz 6 genannten Maßnahmen folgende Kriterien:

a) Schwere und Dauer der Nichteinhaltung;

b) ob die Nichteinhaltung vorsätzlich oder fahrlässig begangen wurde;

c) das Ausmaß der Zusammenarbeit des IKT-Drittdienstleisters mit der federführenden Überwachungsbehörde.

Für die Zwecke des Unterabsatzes 1 führt die federführende Überwachungsbehörde Konsultationen im Rahmen des JON durch, um einen konsistenten Ansatz sicherzustellen.

(9) Zwangsgelder sind administrativer Art und vollstreckbar. Die Zwangsvollstreckung erfolgt nach den geltenden Vorschriften des Zivilprozessrechts des Mitgliedstaats, in dessen Hoheitsgebiet Inspektionen und Zugang erfolgen. Die Gerichte des betreffenden Mitgliedstaats sind für Beschwerden im Zusammenhang mit vorschriftswidrigem Vollzug zuständig. Die Beträge der Zwangsgelder werden dem Gesamthaushaltsplan der Europäischen Union zugewiesen.

(10) Die federführende Überwachungsbehörde veröffentlicht sämtliche verhängten Zwangsgelder, sofern dies die Stabilität der Finanzmärkte nicht ernsthaft gefährdet und den Beteiligten daraus kein unverhältnismäßiger Schaden erwächst.

(11) Die federführende Überwachungsbehörde gibt den Vertretern des dem Verfahren unterliegenden kritischen IKT-Drittdienstleisters vor Verhängung eines Zwangsgeldes nach Absatz 6 Gelegenheit, zu den Feststellungen angehört zu werden, und stützt ihre Entscheidungen ausschließlich auf Feststellungen, zu denen sich der vom Verfahren betroffene kritische IKT-Drittdienstleister äußern konnte.

Die Verteidigungsrechte der vom Verfahren betroffenen Personen werden während des Verfahrens in vollem Umfang gewahrt. Der dem Verfahren unterworfene IKT-Drittdienstleister hat, vorbehaltlich des berechtigten Interesses anderer Personen an der Wahrung ihrer Geschäftsgeheimnisse, ein Recht auf Akteneinsicht. Vom Recht auf Akteneinsicht ausgenommen sind vertrauliche Informationen sowie interne vorbereitende Unterlagen der federführenden Überwachungsbehörde.

*Artikel 36*

**Ausübung der Befugnisse der federführenden Überwachungsbehörde außerhalb der Union**

(1) Wenn sich die Überwachungsziele im Wege der Interaktion mit dem für die Zwecke des Artikels 31 Absatz 12 gegründeten Tochterunternehmen oder durch Überwachungstätigkeiten an Standorten in der Union nicht erreichen lassen, kann die federführende Überwachungsbehörde an allen Standorten in einem Drittland, die sich im Eigentum eines kritischen IKT-Drittdienstleisters befinden oder von ihm zur Erbringung von Dienstleistungen für Finanzunternehmen der Union in irgendeiner Weise im Zusammenhang mit seiner Geschäftstätigkeit, seinen Funktionen oder seinen Dienstleistungen genutzt werden, wozu alle Verwaltungs-, Geschäfts- oder Betriebsstellen, Räumlichkeiten, Grundstücke, Gebäude oder andere Immobilien gehören, die Befugnisse ausüben, die in folgenden Bestimmungen genannt werden:

a) in Artikel 35 Absatz 1 Buchstabe a und

b) in Artikel 35 Absatz 1 Buchstabe b im Einklang mit Artikel 38 Absatz 2 Buchstaben a, b und d sowie in Artikel 39 Absatz 1 und Absatz 2 Buchstabe a.

Die in Unterabsatz 1 genannten Befugnisse können unter den folgenden Bedingungen ausgeübt werden:

i) Die federführende Überwachungsbehörde erachtet die Durchführung einer Inspektion in einem Drittland als notwendig, damit sie ihre Aufgaben entsprechend dieser Verordnung vollständig und wirksam wahrnehmen kann;

ii) die Inspektion in einem Drittland steht in direktem Zusammenhang mit der Bereitstellung von IKT-Dienstleistungen für Finanzunternehmen in der Union;

iii) der betreffende kritische IKT-Drittdienstleister stimmt der Durchführung einer Inspektion in einem Drittland zu; und

iv) die einschlägige Behörde des betreffenden Drittlands wurde von der federführenden Überwachungsbehörde offiziell unterrichtet und hat keine Einwände dagegen erhoben.

(2) Unbeschadet der jeweiligen Zuständigkeiten der Organe der Union und der Mitgliedstaaten schließen die EBA, die ESMA oder die EIOPA für die Zwecke des Absatzes 1 Vereinbarungen über die Verwaltungszusammenarbeit mit der einschlägigen Behörde des Drittlands, um die reibungslose Durchführung von Inspektionen in dem betreffenden Drittland durch die federführende Überwachungsbehörde und ihr für ihren Auftrag in diesem Drittland benanntes Team zu ermöglichen. Diese Kooperationsvereinbarungen begründen keine rechtlichen Verpflichtungen gegenüber der Union und ihren Mitgliedstaaten und hindern die Mitgliedstaaten und ihre zuständigen Behörden nicht daran, bilaterale oder multilaterale Vereinbarungen mit diesen Drittländern und deren einschlägigen Behörden zu schließen.

In den Kooperationsvereinbarungen sind mindestens die folgenden Elemente festgelegt:

a) die Verfahren für die Koordinierung der im Rahmen dieser Verordnung durchgeführten Überwachungstätigkeiten und jede entsprechende Überwachung des IKT-Drittparteienrisikos im Finanzsektor durch die einschlägige Behörde des betreffenden Drittlands, einschließlich der Einzelheiten für die Übermittlung der Zustimmung dieser Behörde, damit die federführende Überwachungsbehörde und ihr benanntes Team in dessen Hoheitsgebiet allgemeine Untersuchungen und Vor-Ort-Inspektionen gemäß Absatz 1 Unterabsatz 1 durchführen können;

b) der Mechanismus für die Übermittlung aller relevanten Informationen zwischen der EBA, der ESMA oder der EIOPA und der einschlägigen Behörde des betreffenden Drittlands, insbesondere im Zusammenhang mit Informationen, die von der federführenden Überwachungsbehörde gemäß Artikel 37 angefordert werden können;

c) die Mechanismen für die unverzügliche Unterrichtung der EBA, der ESMA oder der EIOPA durch die einschlägige Behörde des betreffenden Drittlands über Fälle, in denen einem IKT-Drittdienstleister mit Sitz in einem Drittland, der gemäß Artikel 31 Absatz 1 Buchstabe a als kritisch eingestuft wurde, ein Verstoß gegen die Anforderungen zur Last gelegt wird, die er nach dem geltenden Recht des betreffenden Drittlands bei der Erbringung von Dienstleistungen für Finanzinstitute in diesem Drittland einhalten muss, sowie die angewandten Rechtsbehelfe und verhängten Sanktionen;

d) die regelmäßige Übermittlung von Neuerungen im Bereich der regulatorischen und aufsichtlichen Entwicklungen bei der Überwachung des IKT-Drittparteienrisikos für Finanzinstitute in dem betreffenden Drittland;

e) die Einzelheiten, die erforderlichenfalls die Teilnahme eines Vertreters der zuständigen Drittlandsbehörde an den Inspektionen der federführenden Überwachungsbehörde und des benannten Teams ermöglichen.

(3) Ist die federführende Überwachungsbehörde nicht in der Lage, die in den Absätzen 1 und 2 genannten Überwachungstätigkeiten außerhalb der Union durchzuführen, so

a) übt sie ihre Befugnisse nach Artikel 35 auf der Grundlage aller ihr bekannten Tatsachen und zur Verfügung stehenden Unterlagen aus;

b) dokumentiert und erläutert sie alle Folgen, die sich daraus ergeben, dass sie nicht in der Lage ist, die geplanten Überwachungstätigkeiten gemäß diesem Artikel durchzuführen.

Die in Buchstabe b genannten potenziellen Folgen werden in den Empfehlungen der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d berücksichtigt.

*Artikel 37*

**Auskunftsersuchen**

(1) Die federführende Überwachungsbehörde kann von kritischen IKT-Drittdienstleistern durch einfaches Ersuchen oder durch Beschluss verlangen, alle Informationen zur Verfügung zu stellen, die die federführende Überwachungsbehörde benötigt, um ihre Aufgaben im Rahmen dieser Verordnung wahrzunehmen, einschließlich aller relevanten Geschäfts- oder Betriebsunterlagen, Verträge, Leit- und Richtlinien, Dokumentationen, Meldungen über IKT-Sicherheitsprüfungen, Berichte über IKT-bezogene Vorfälle sowie aller Informationen über Parteien, an die der kritische IKT-Drittdienstleister betriebliche Funktionen oder Tätigkeiten ausgelagert hat.

(2) Bei der Übermittlung eines einfachen Auskunftsersuchens nach Absatz 1 verfährt die federführende Überwachungsbehörde wie folgt:

a) Sie nimmt auf diesen Artikel als Rechtsgrundlage des Ersuchens Bezug;

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert, welche Informationen gefordert werden;

d) sie legt die Frist für die Vorlage der Informationen fest;

e) sie unterrichtet den Vertreter des kritischen IKT-Drittdienstleisters, von dem die Informationen angefordert werden, darüber, dass er zu deren Übermittlung zwar nicht verpflichtet ist, die vorgelegten Informationen bei freiwilliger Beantwortung des Ersuchens jedoch nicht falsch oder irreführend sein dürfen.

(3) Fordert die federführende Überwachungsbehörde durch entsprechenden Beschluss gemäß Absatz 1 Informationen an, verfährt sie wie folgt:

a) Sie nimmt auf diesen Artikel als Rechtsgrundlage des Ersuchens Bezug;

b) sie gibt den Zweck des Ersuchens bekannt;

c) sie erläutert, welche Informationen gefordert werden;

d) sie legt die Frist für die Vorlage der Informationen fest;

e) sie nennt die Zwangsgelder, die nach Artikel 35 Absatz 6 verhängt werden, wenn die geforderten Informationen unvollständig sind oder nicht innerhalb der unter Buchstabe d genannten Frist vorgelegt werden;

f) sie weist auf das Recht nach den Artikeln 60 und 61 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 hin, vor dem Beschwerdeausschuss der ESA Beschwerde gegen den Beschluss einzulegen und den Beschluss durch den Gerichtshof der Europäischen Union (im Folgenden „Gerichtshof") überprüfen zu lassen.

(4) Die Vertreter der kritischen IKT-Drittdienstleister stellen die angeforderten Informationen zur Verfügung. Ordnungsgemäß bevollmächtigte Rechtsanwälte können die Auskünfte im Namen ihrer Mandanten erteilen. Die kritischen IKT-Drittdienstleister bleiben in vollem Umfang verantwortlich, wenn die erteilten Auskünfte unvollständig, sachlich unrichtig oder irreführend sind.

(5) Die federführende Überwachungsbehörde übermittelt den für diejenigen Finanzunternehmen, die die Dienste der betreffenden kritischen IKT-Drittdienstleister nutzen, zuständigen Behörden sowie dem JON unverzüglich eine Kopie der Entscheidung, Informationen bereitzustellen.

*Artikel 38*

**Allgemeine Untersuchungen**

(1) Die federführende Überwachungsbehörde kann zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung mit Unterstützung des in Artikel 40 Absatz 1 genannten gemeinsamen Untersuchungsteams erforderlichenfalls Untersuchungen von kritischen IKT-Drittdienstleistern durchführen.

(2) Die federführende Überwachungsbehörde ist befugt,

a) Aufzeichnungen, Daten, Verfahren und sonstiges für die Erfüllung ihrer Aufgaben relevantes Material unabhängig von der Speicherform zu prüfen;

b) beglaubigte Kopien oder Auszüge dieser Aufzeichnungen, Daten und dokumentierten Verfahren und von sämtlichen sonstigen Materialien anzufertigen oder zu verlangen;

c) Vertreter des kritischen IKT-Drittdienstleisters vorzuladen und zur Abgabe mündlicher oder schriftlicher Erklärungen zu Sachverhalten oder Unterlagen aufzufordern, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, und die Antworten aufzuzeichnen;

d) jede andere natürliche oder juristische Person zu befragen, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

e) Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern.

(3) Die Bediensteten und sonstige von der federführenden Überwachungsbehörde zu Untersuchungen gemäß Absatz 1 ermächtigte Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Ermächtigung aus, in der Gegenstand und Zweck der Untersuchung angegeben werden.

In der Ermächtigung sind auch die in Artikel 35 Absatz 6 vorgesehenen Zwangsgelder für den Fall anzugeben, dass die angeforderten Aufzeichnungen, Daten, dokumentierten Verfahren oder sonstigen Materialien oder die Antworten auf Fragen, die den Vertretern des IKT-Drittdienstleisters gestellt werden, nicht geliefert werden oder unvollständig sind.

(4) Die Vertreter der kritischen IKT-Drittdienstleister sind verpflichtet, sich den Untersuchungen auf der Grundlage einer Entscheidung der federführenden Überwachungsbehörde zu unterziehen. In dem Beschluss sind Gegenstand und Zweck der Untersuchung, die nach Artikel 35 Absatz 6 vorgesehenen Zwangsgelder, die nach den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 möglichen Rechtsbehelfe sowie das Recht, den Beschluss durch den Gerichtshof überprüfen zu lassen, anzugeben.

(5) Rechtzeitig vor Beginn der Untersuchung unterrichtet die federführende Überwachungsbehörde die für diejenigen Finanzunternehmen, die die IKT-Dienstleistungen dieses kritischen IKT-Drittdienstleisters nutzen, zuständigen Behörden über die geplante Untersuchung sowie die Identität der bevollmächtigten Personen.

Die federführende Überwachungsbehörde übermittelt dem JON alle gemäß Unterabsatz 1 mitgeteilten Informationen.

*Artikel 39*

**Inspektionen**

(1) Die federführende Überwachungsbehörde kann zur Wahrnehmung ihrer Aufgaben nach dieser Verordnung mit Unterstützung der in Artikel 40 Absatz 1 genannten gemeinsamen Untersuchungsteams sämtliche Geschäftsräume, Grundstücke oder Gebäude des IKT-Drittdienstleisters, wie Hauptverwaltungen, Betriebszentren und sekundäre Räumlichkeiten, betreten und dort alle erforderlichen Vor-Ort-Inspektionen durchführen sowie außerhalb dieser Räumlichkeiten Inspektionen durchführen.

Für die Ausübung der in Unterabsatz 1 genannten Befugnisse konsultiert die federführende Überwachungsbehörde das JON.

(2) Die Bediensteten und sonstige Personen, die von der federführenden Überwachungsbehörde zur Durchführung einer Vor-Ort-Inspektion ermächtigt wurden, sind befugt,

a) diese Geschäftsräume, Grundstücke oder Gebäude zu betreten; und

b) diese Geschäftsräume, Bücher oder Aufzeichnungen für die Dauer der Inspektion und in dem für die Inspektion erforderlichen Umfang zu versiegeln.

Die Bediensteten und sonstige von der federführenden Überwachungsbehörde ermächtigten Personen üben ihre Befugnisse unter Vorlage einer schriftlichen Ermächtigung aus, in der Gegenstand und Zweck der Inspektion sowie die in Artikel 35 Absatz 6 vorgesehenen Zwangsgelder angegeben sind, die verhängt werden, wenn sich die Vertreter der betreffenden IKT-Drittdienstleister der Inspektion nicht unterziehen.

(3) Die federführende Überwachungsbehörde unterrichtet die für diejenigen Finanzunternehmen, die diesen IKT-Drittdienstleister in Anspruch nehmen, zuständigen Behörden rechtzeitig vor der Inspektion.

(4) Die Inspektionen erstrecken sich auf das gesamte Spektrum einschlägiger IKT-Systeme, -Netzwerke, -Geräte, -Informationen und -Daten, die für die Erbringung von IKT-Dienstleistungen für Finanzunternehmen verwendet werden oder dazu beitragen.

(5) Die federführende Überwachungsbehörde unterrichtet die kritischen IKT-Drittdienstleister vor jeder geplanten Vor-Ort-Inspektion mit angemessenem Vorlauf, es sei denn, eine solche Unterrichtung ist aufgrund einer Not- oder Krisensituation nicht möglich oder würde Umstände herbeiführen, unter denen die Inspektion oder das Audit nicht mehr wirksam wären.

(6) Der kritische IKT-Drittdienstleister unterzieht sich den durch Beschluss der federführenden Überwachungsbehörde angeordneten Vor-Ort-Inspektionen. In dem Beschluss sind Gegenstand, Zweck und Datum des Beginns der Inspektion, die nach Artikel 35 Absatz 6 vorgesehenen Zwangsgelder, die nach den Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 möglichen Rechtsbehelfe sowie das Recht, den Beschluss durch den Gerichtshof überprüfen zu lassen, anzugeben.

(7) Gelangen die Bediensteten und sonstige von der federführenden Überwachungsbehörde bevollmächtigte Personen zu dem Schluss, dass ein kritischer IKT-Drittdienstleister sich einer gemäß diesem Artikel angeordneten Inspektion widersetzt, unterrichtet die federführende Überwachungsbehörde den kritischen IKT-Drittdienstleister über die Folgen einer solchen Widersetzung, einschließlich der Möglichkeit der für die betreffenden Finanzunternehmen zuständigen Behörden, Finanzunternehmen zu verpflichten, die mit diesem kritischen IKT-Drittdienstleister geschlossenen vertraglichen Vereinbarungen zu kündigen.

*Artikel 40*

**Laufende Überwachung**

(1) Bei der Durchführung von Überwachungstätigkeiten, insbesondere allgemeinen Untersuchungen oder Inspektionen, wird die federführende Überwachungsbehörde von einem gemeinsamen Untersuchungsteam unterstützt, das für jeden kritischen IKT-Drittdienstleister eingerichtet wird.

(2) Das in Absatz 1 genannte gemeinsame Untersuchungsteam setzt sich aus Mitarbeitern der folgenden Behörden zusammen:

a) der ESA;

b) der jeweils zuständigen Behörden, die die Finanzunternehmen beaufsichtigen, denen der kritische IKT-Drittdienstleister IKT-Dienstleistungen erbringt;

c) der in Artikel 32 Absatz 4 Buchstabe e genannten zuständigen nationale Behörde, auf freiwilliger Basis;

d) einer zuständigen nationalen Behörde des Mitgliedstaats, in dem der kritische IKT-Drittdienstleister seinen Sitz hat, auf freiwilliger Basis.

Die Mitglieder des gemeinsamen Untersuchungsteams müssen über Fachwissen in den Bereichen IKT und operationelle Risiken verfügen. Das gemeinsame Untersuchungsteam arbeitet unter der Koordinierung eines benannten Mitarbeiters der federführenden Überwachungsbehörde („Koordinator der federführenden Überwachungsbehörde“).

(3) Innerhalb von 3 Monaten nach Abschluss einer Untersuchung oder Inspektion nimmt die federführende Überwachungsbehörde nach Konsultation des Überwachungsforums entsprechend den in Artikel 35 genannten Befugnissen an den kritischen IKT-Drittdienstleister zu richtende Empfehlungen an.

(4) Die in Absatz 3 genannten Empfehlungen werden dem kritischen IKT-Drittdienstleister und den für diejenigen Finanzunternehmen, denen er IKT-Dienstleistungen erbringt, zuständigen Behörden unverzüglich übermittelt.

Die federführende Überwachungsbehörde kann zur Erfüllung der Überwachungstätigkeiten alle einschlägigen Zertifizierungen Dritter und interne oder externe IKT-Prüfungsberichte Dritter berücksichtigen, die von dem kritischen IKT-Drittdienstleister zur Verfügung gestellt werden.

*Artikel 41*

**Harmonisierung der Voraussetzungen für die Durchführung der Überwachungstätigkeiten**

(1) Die ESA arbeiten über den Gemeinsamen Ausschuss Entwürfe technischer Regulierungsstandards aus, um Folgendes festzulegen:

a) die Informationen, die von einem IKT-Drittdienstleister in dem Antrag bereitzustellen sind, in dem gemäß Artikel 31 Absatz 11 freiwillig um Einstufung als kritisch ersucht wird;

b) Inhalt, Struktur und Format der Informationen, die IKT-Drittdienstleister gemäß Artikel 35 Absatz 1 übermitteln, offenlegen und melden müssen, einschließlich der Vorlage für die Bereitstellung von Informationen über die Vereinbarungen über die Unterauftragsvergabe;

c) die Kriterien für die Festlegung der Zusammensetzung des gemeinsamen Untersuchungsteams, bei der eine ausgewogene Beteiligung der Mitarbeiter der ESA und der jeweils zuständigen Behörden sicherzustellen ist, sowie ihrer Benennung, Aufgaben und Arbeitsvereinbarungen;

d) die Einzelheiten der von den zuständigen Behörden vorgenommenen Bewertung der Maßnahmen, die von kritischen IKT-Drittdienstleistern auf der Grundlage der Empfehlungen der federführenden Überwachungsbehörde gemäß Artikel 42 Absatz 3 ergriffen wurden.

(2) Die ESA legen der Kommission diese Entwürfe technischer Regulierungsstandards bis zum 17. Juli 2024 vor.

Der Kommission wird die Befugnis übertragen, die vorliegende Verordnung durch Annahme technischer Regulierungsstandards nach Absatz 1 entsprechend dem Verfahren nach den Artikeln 10 bis 14 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1094/2010 und (EU) Nr. 1095/2010 zu ergänzen.

*Artikel 42*

**Folgemaßnahmen zuständiger Behörden**

(1) Kritische IKT-Drittdienstleister teilen entweder der federführenden Überwachungsbehörde innerhalb von 60 Kalendertagen nach Eingang der Empfehlungen, die von der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d abgegeben werden, ihre Absicht mit, diesen Empfehlungen Folge zu leisten, oder legen eine begründete Erklärung für die Nichtbefolgung der Empfehlungen vor. Die federführende Überwachungsbehörde übermittelt diese Informationen unverzüglich den für das betreffende Finanzunternehmen zuständigen Behörden.

(2) Die federführende Überwachungsbehörde informiert öffentlich darüber, wenn ein kritischer IKT-Drittdienstleister es versäumt, die federführende Überwachungsbehörde gemäß Absatz 1 zu unterrichten, oder wenn die Erklärung des kritischen IKT-Drittdienstleisters als nicht ausreichend erachtet wird. Die veröffentlichten Informationen enthalten die Identität des kritischen IKT-Drittdienstleisters sowie Angaben über Art und Wesen der Nichtkonformität. Diese Informationen werden auf den zum Zweck der Gewährleistung der Sensibilisierung der Öffentlichkeit relevanten und angemessenen Umfang beschränkt, es sei denn eine solche Veröffentlichung würde den Beteiligten einen unverhältnismäßigen Schaden zufügen oder das ordnungsgemäße Funktionieren und die Integrität von Finanzmärkten oder die Stabilität des Finanzsystems der Union als Ganzes oder in Teilen gefährden.

Die federführende Überwachungsbehörde unterrichtet den IKT-Drittdienstleister über diese Veröffentlichung.

(3) Die zuständigen Behörden unterrichten die betreffenden Finanzunternehmen über die Risiken, die in den Empfehlungen an kritische IKT-Drittdienstleister gemäß Artikel 35 Absatz 1 Buchstabe d festgestellt wurden.

Beim Management des IKT-Drittparteienrisikos berücksichtigen die Finanzunternehmen die in Unterabsatz 1 genannten Risiken.

(4) Ist eine zuständige Behörde der Ansicht, dass ein Finanzunternehmen die in den Empfehlungen festgestellten spezifischen Risiken bei seinem Management der IKT-Drittparteienrisiken nicht oder nicht ausreichend berücksichtigt, teilt sie dem Finanzunternehmen mit, dass innerhalb von 60 Kalendertagen nach Eingang einer solchen Mitteilung eine Entscheidung gemäß Absatz 6 getroffen werden kann, falls keine geeigneten vertraglichen Vereinbarungen zur Beseitigung dieser Risiken bestehen.

(5) Nach Eingang der in Artikel 35 Absatz 1 Buchstabe c genannten Berichte und vor einer Entscheidung gemäß Absatz 6 können die zuständigen Behörden auf freiwilliger Basis die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden konsultieren, die für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig sind.

(6) Im Einklang mit Artikel 50 können zuständige Behörden als letztes Mittel nach der Mitteilung und gegebenenfalls der Abstimmung gemäß den Absätzen 4 und 5 eine Entscheidung treffen, mit der sie von Finanzunternehmen verlangen, die Nutzung oder den Einsatz einer Dienstleistung, die von einem kritischen IKT-Drittdienstleister bereitgestellt wird, vorübergehend teilweise oder vollständig auszusetzen, bis die Risiken beseitigt sind, die in den an den kritischen IKT-Drittdienstleister gerichteten Empfehlungen festgestellt wurden. Die Behörden können von Finanzunternehmen erforderlichenfalls verlangen, die einschlägigen vertraglichen Vereinbarungen, die mit kritischen IKT-Drittdienstleistern geschlossen wurden, ganz oder teilweise zu kündigen.

(7) Verweigert ein kritischer IKT-Drittdienstleister die Befolgung der Empfehlungen, indem er einen anderen als den von der federführenden Überwachungsbehörde empfohlenen Ansatz wählt, und wirkt sich ein solcher abweichender Ansatz möglicherweise auf eine große Zahl von Finanzunternehmen oder einen erheblichen Teil des Finanzsektors negativ aus und haben einzelne Warnungen der zuständigen Behörden nicht zu kohärenten Ansätzen geführt, die das potenzielle Risiko für die Finanzstabilität mindern, kann die federführende Überwachungsbehörde nach Konsultation des Überwachungsforums den zuständigen Behörden gegebenenfalls unverbindliche und nicht für die Öffentlichkeit bestimmte Stellungnahmen übermitteln, um kohärente und konvergente aufsichtliche Folgemaßnahmen zu fördern.

(8) Nach Eingang der in Artikel 35 Absatz 1 Buchstabe c genannten Berichte berücksichtigen die zuständigen Behörden bei der in Absatz 6 genannten Entscheidung die Art und das Ausmaß des Risikos, das vom kritischen IKT-Drittdienstleister nicht angegangen wird, sowie die Schwere des Verstoßes unter Berücksichtigung der folgenden Kriterien:

a) der Schwere und Dauer des Verstoßes;

b) ob durch den Verstoß schwerwiegende Mängel in Bezug auf Verfahren, Managementsysteme, Risikomanagement und interne Kontrollen des kritischen IKT-Drittdienstleisters offengelegt wurden;

c) ob Wirtschaftskriminalität erleichtert oder herbeigeführt wurde oder auf andere Weise mit dem Verstoß in Verbindung steht;

d) ob der Verstoß vorsätzlich oder fahrlässig begangen wurde;

e) ob die Aussetzung oder Kündigung der vertraglichen Vereinbarungen ungeachtet der Bemühungen des Finanzunternehmens um Vermeidung von Störungen bei der Erbringung seiner Dienstleistungen ein Risiko für die Fortführung der Geschäftstätigkeit des Finanzunternehmens mit sich bringt;

f) gegebenenfalls der gemäß Absatz 5 auf freiwilliger Basis ersuchten Stellungnahme der gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden, die für die Beaufsichtigung eines wesentlichen oder wichtigen, von der genannten Richtlinie erfassten Unternehmens, das als kritischer IKT-Drittdienstleister eingestuft wurde, zuständig sind.

Die zuständigen Behörden gewähren Finanzunternehmen den erforderlichen Zeitraum, damit sie die vertraglichen Vereinbarungen mit kritischen IKT-Drittdienstleistern anpassen können, um nachteilige Auswirkungen auf ihre digitale operationale Resilienz zu vermeiden und ihnen die Anwendung der in Artikel 28 genannten Ausstiegsstrategien und Übergangspläne zu ermöglichen.

(9) Die Entscheidung gemäß Absatz 6 wird den in Artikel 32 Absatz 4 Buchstaben a, b und c genannten Mitgliedern des Überwachungsforums und dem JON mitgeteilt.

Die von den Entscheidungen gemäß Absatz 6 betroffenen kritischen IKT-Drittdienstleister arbeiten uneingeschränkt mit den betroffenen Finanzunternehmen zusammen, insbesondere im Zusammenhang mit dem Verfahren zur Aussetzung oder Kündigung ihrer vertraglichen Vereinbarungen.

(10) Die zuständigen Behörden unterrichten die federführende Überwachungsbehörde regelmäßig über die Herangehensweisen und Maßnahmen, die sie bei ihren Aufsichtsaufgaben in Bezug auf Finanzunternehmen gewählt haben, sowie über die von den Finanzunternehmen geschlossenen vertraglichen Vereinbarungen, wenn kritische IKT-Drittdienstleister Empfehlungen, die von der federführenden Überwachungsbehörde an sie gerichtet wurden, teilweise oder vollständig nicht befolgt haben.

(11) Die federführende Überwachungsbehörde kann auf Verlangen die zur Anleitung der zuständigen Behörden abgegebenen Empfehlungen näher erläutern.

*Artikel 43*

**Überwachungsgebühren**

(1) Die federführende Überwachungsbehörde erhebt gemäß dem in Absatz 2 genannten delegierten Rechtsakt von kritischen IKT-Drittdienstleistern Gebühren, die die notwendigen Ausgaben der federführenden Überwachungsbehörde für die Durchführung von Überwachungsaufgaben gemäß dieser Verordnung vollständig decken, einschließlich der Erstattung aller Kosten, die durch die Arbeit des in Artikel 40 genannten gemeinsamen Untersuchungsteams entstehen können, sowie der Kosten für die Beratung durch die in Artikel 32 Absatz 4 Unterabsatz 2 genannten unabhängigen Sachverständigen in Angelegenheiten, die in den Aufgabenbereich der direkten Überwachungstätigkeiten fallen.

Die Höhe einer Gebühr, die einem kritischen IKT-Drittdienstleister in Rechnung gestellt wird, deckt alle Kosten ab, die aufgrund der Erfüllung der in diesem Abschnitt festgelegten Aufgaben anfallen, und steht in einem angemessenen Verhältnis zu dessen Umsatz.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 57 einen delegierten Rechtsakt zur Ergänzung dieser Verordnung durch Festlegung der Höhe der Gebühren und der Art und Weise ihrer Entrichtung bis zum 17. Juli 2024 zu erlassen.

*Artikel 44*

**Internationale Zusammenarbeit**

(1) Unbeschadet des Artikels 36 können die EBA, die ESMA und die EIOPA im Einklang mit Artikel 33 der Verordnungen (EU) Nr. 1093/2010, (EU) Nr. 1095/2010 bzw. (EU) Nr. 1094/2010 Verwaltungsvereinbarungen mit Regulierungs- und Überwachungsbehörden von Drittländern schließen, um die internationale Zusammenarbeit in Bezug auf das IKT-Drittparteienrisiko in verschiedenen Finanzsektoren zu fördern, insbesondere durch die Entwicklung bewährter Verfahren für die Überprüfung von IKT-Risikomanagementverfahren und -kontrollen, Abmilderungsmaßnahmen und Reaktionsmaßnahmen bei Vorfällen.

(2) Die ESA legen dem Europäischen Parlament, dem Rat und der Kommission über den Gemeinsamen Ausschuss alle fünf Jahre einen gemeinsamen vertraulichen Bericht vor, in dem die Ergebnisse einschlägiger Gespräche mit den in Absatz 1 genannten Behörden von Drittländern zusammengefasst werden, wobei der Schwerpunkt auf der Entwicklung des IKT-Drittparteienrisikos und den Auswirkungen auf die Finanzstabilität, die Marktintegrität, den Anlegerschutz und das Funktionieren des Binnenmarkts liegt.

***KAPITEL VI***

***Vereinbarungen über den Austausch von Informationen***

*Artikel 45*

**Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen**

(1) Finanzunternehmen können Informationen und Erkenntnisse über Cyberbedrohungen untereinander austauschen, einschließlich Indikatoren für Beeinträchtigungen, Taktiken, Techniken und Verfahren, Cybersicherheitswarnungen und Konfigurationstools, soweit dieser Austausch von Informationen und Erkenntnissen

a) darauf abzielt, die digitale operationale Resilienz von Finanzunternehmen zu stärken, insbesondere indem für Cyberbedrohungen sensibilisiert, die Verbreitung von Cyberbedrohungen eingeschränkt oder verhindert wird und die Verteidigungsfähigkeiten, Techniken zur Erkennung von Bedrohungen, Abmilderungsstrategien oder Phasen der Reaktion und Wiederherstellung unterstützt werden;

b) innerhalb vertrauenswürdiger Gemeinschaften von Finanzunternehmen erfolgt;

c) durch Vereinbarungen über den Austausch von Informationen umgesetzt wird, die den potenziell sensiblen Charakter der ausgetauschten Informationen schützen und Verhaltensregeln unterliegen, in deren Rahmen die Wahrung des Geschäftsgeheimnisses, der Schutz personenbezogener Daten im Einklang mit der Verordnung (EU) 2016/679 und Leitlinien für die Wettbewerbspolitik vollumfänglich befolgt werden.

(2) Für die Zwecke von Absatz 1 Buchstabe c werden in den Vereinbarungen über den Austausch von Informationen die Voraussetzungen für die Teilnahme und gegebenenfalls die Einzelheiten zur Einbindung staatlicher Behörden und der Eigenschaft, in der diese in die Vereinbarungen über den Austausch von Informationen eingebunden werden können, zur Einbindung von IKT-Drittdienstleistern sowie zu operativen Aspekten, einschließlich der Nutzung spezieller IT-Plattformen, festgelegt.

(3) Finanzunternehmen teilen zuständigen Behörden ihre Einbindung in die in Absatz 1 genannten Vereinbarungen über den Austausch von Informationen mit, sobald ihre Mitwirkung bestätigt wurde bzw. endet und diese Beendigung in Kraft ist.

*KAPITEL VII*

***Zuständige Behörden***

*Artikel 46*

**Zuständige Behörden**

Unbeschadet der Bestimmungen über den Überwachungsrahmen für kritische IKT-Drittdienstleister gemäß Kapitel V Abschnitt II dieser Verordnung wird die Einhaltung dieser Verordnung durch die folgenden zuständigen Behörden im Einklang mit den durch die jeweiligen Rechtsakte übertragenen Befugnissen sichergestellt:

a) bei Kreditinstituten sowie bei nach der Richtlinie 2013/36/EU ausgenommenen Instituten durch die gemäß Artikel 4 der genannten Richtlinie benannte zuständige Behörde und bei gemäß Artikel 6 Absatz 4 der Verordnung (EU) Nr. 1024/2013 als bedeutend eingestuften Kreditinstituten durch die EZB im Einklang mit den mittels der genannten Verordnung übertragenen Befugnissen und Aufgaben;

b) bei Zahlungsinstituten, einschließlich der nach der Richtlinie (EU) 2015/2366 ausgenommenen Zahlungsinstitute, bei E-Geld-Instituten, einschließlich der nach der Richtlinie 2009/110/EG ausgenommenen Institute, und bei den in Artikel 33 Absatz 1 der Richtlinie (EU) 2015/2366 genannten Kontoinformationsdienstleistern durch die gemäß Artikel 22 der Richtlinie (EU) 2015/2366 benannte zuständige Behörde;

c) bei Wertpapierfirmen durch die gemäß Artikel 4 der Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates ([38]) benannte zuständige Behörde;

d) bei gemäß der Verordnung über Märkte von Krypto-Werten zugelassenen Anbietern von Krypto-Dienstleistungen und Emittenten von an Vermögenswerte geknüpften Tokens durch die gemäß der entsprechenden Bestimmung der genannten Verordnung benannte zuständige Behörde;

e) bei Zentralverwahrern durch die gemäß Artikel 11 der Verordnung (EU) Nr. 909/2014 benannte zuständige Behörde;

f) bei zentralen Gegenparteien durch die gemäß Artikel 22 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

g) bei Handelsplätzen und Datenbereitstellungsdiensten durch die gemäß Artikel 67 der Richtlinie 2014/65/EU benannte zuständige Behörde und die zuständige Behörde im Sinne von Artikel 2 Absatz 1 Nummer 18 der Verordnung (EU) Nr. 600/2014;

h) bei Transaktionsregistern durch die gemäß Artikel 22 der Verordnung (EU) Nr. 648/2012 benannte zuständige Behörde;

i) bei Verwaltern alternativer Investmentfonds durch die gemäß Artikel 44 der Richtlinie 2011/61/EU benannte zuständige Behörde;

j) bei Verwaltungsgesellschaften durch die gemäß Artikel 97 der Richtlinie 2009/65/EG benannte zuständige Behörde;

k) bei Versicherungs- und Rückversicherungsunternehmen durch die gemäß Artikel 30 der Richtlinie 2009/138/EG benannte zuständige Behörde;

l) bei Versicherungsvermittlern, Rückversicherungsvermittlern und Versicherungsvermittlern in Nebentätigkeit durch die gemäß Artikel 12 der Richtlinie (EU) 2016/97 benannte zuständige Behörde;

m) bei Einrichtungen der betrieblichen Altersversorgung durch die gemäß Artikel 47 der Richtlinie (EU) 2016/2341 benannte zuständige Behörde;

n) bei Ratingagenturen durch die gemäß Artikel 21 der Verordnung (EG) Nr. 1060/2009 benannte zuständige Behörde;

o) bei Administratoren kritischer Referenzwerte durch die gemäß den Artikeln 40 und 41 der Verordnung (EU) 2016/1011 benannte zuständige Behörde;

([38]) Richtlinie (EU) 2019/2034 des Europäischen Parlaments und des Rates vom 27. November 2019 über die Beaufsichtigung von Wertpapierfirmen und zur Änderung der Richtlinien 2002/87/EG, 2009/65/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU und 2014/65/EU (ABl. L 314 vom 5.12.2019, S. 64).

p) bei Schwarmfinanzierungsdienstleistern durch die gemäß Artikel 29 der Verordnung (EU) 2020/1503 benannte zuständige Behörde;

q) bei Verbriefungsregistern durch die gemäß Artikel 10 und Artikel 14 Absatz 1 der Verordnung (EU) 2017/2402 benannte zuständige Behörde.

*Artikel 47*

**Zusammenarbeit mit den durch die Richtlinie (EU) 2022/2555 geschaffenen Strukturen und Behörden**

(1) Um die Zusammenarbeit zu fördern und den aufsichtlichen Austausch zwischen den gemäß dieser Verordnung benannten zuständigen Behörden und der durch Artikel 14 der Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe zu ermöglichen, können sich die ESA und die zuständigen Behörden bei Angelegenheiten, die ihre Aufsichtstätigkeiten in Bezug auf Finanzunternehmen betreffen, an den Tätigkeiten der Kooperationsgruppe beteiligen. Die ESA und die zuständigen Behörden können verlangen, zur Teilnahme an den Tätigkeiten der Kooperationsgruppe in Angelegenheiten im Zusammenhang mit den wesentlichen oder wichtigen, von der Richtlinie (EU) 2022/2555 erfassten Unternehmen, die ebenfalls gemäß Artikel 31 der vorliegenden Verordnung als kritische IKT-Drittdienstleister eingestuft wurden, eingeladen zu werden.

(2) Die zuständigen Behörden können sich gegebenenfalls an die zentralen Anlaufstellen und die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten CSIRT wenden und mit ihnen Informationen austauschen.

(3) Die zuständigen Behörden können gegebenenfalls die gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden um einschlägige fachliche Beratung und Unterstützung ersuchen und Kooperationsvereinbarungen schließen, um die Einrichtung wirksamer und schneller Koordinierungsmechanismen zu ermöglichen.

(4) In den in Absatz 3 genannten Vereinbarungen können unter anderem Verfahren für die Koordinierung der Aufsichts- bzw. Überwachungstätigkeiten in Bezug auf wesentliche oder wichtige, von der Richtlinie (EU) 2022/2555 erfasste Unternehmen, die gemäß Artikel 31 der vorliegenden Verordnung als kritische IKT-Drittdienstleister eingestuft wurden, festgelegt werden, wozu die Durchführung von Untersuchungen und Vor-Ort-Inspektionen im Einklang mit dem nationalen Recht sowie Mechanismen für den Informationsaustausch zwischen den gemäß der vorliegenden Verordnung zuständigen Behörden und den gemäß der genannten Richtlinie benannten oder eingerichteten Behörden, einschließlich des Zugangs zu den von den letztgenannten Behörden angeforderten Informationen, gehören.

*Artikel 48*

**Zusammenarbeit der Behörden**

(1) Die zuständigen Behörden arbeiten untereinander und gegebenenfalls mit der federführenden Überwachungsbehörde eng zusammen.

(2) Die zuständigen Behörden und die federführende Überwachungsbehörde tauschen zeitnah alle relevanten Informationen über kritische IKT-Drittdienstleister aus, die sie benötigen, um ihre jeweiligen Aufgaben gemäß dieser Verordnung wahrnehmen zu können, insbesondere in Bezug auf die ermittelten Risiken, die Herangehensweisen und die Maßnahmen, die im Rahmen der Überwachungsaufgaben der federführenden Überwachungsbehörde ergriffen wurden.

*Artikel 49*

**Sektorübergreifende Übungen, Kommunikation und Zusammenarbeit im Finanzbereich**

(1) Die ESA können über den Gemeinsamen Ausschuss und in Zusammenarbeit mit — je nach Sachlage — den zuständigen Behörden, den in Artikel 3 der Richtlinie 2014/59/EU genannten nationalen Abwicklungsbehörden, der EZB, dem Einheitlichen Abwicklungsausschuss (bei Informationen über Unternehmen, die in den Geltungsbereich der Verordnung (EU) Nr. 806/2014 fallen), dem ESRB und der ENISA Mechanismen für den Austausch wirksamer Verfahren zwischen Finanzsektoren einrichten, um die Lageerfassung zu verbessern und sektorübergreifend gemeinsame Cyberanfälligkeiten und -risiken zu ermitteln.

Ebenso können sie Krisenmanagement- und Notfallübungen mit Szenarien für Cyberangriffe konzipieren, um Kommunikationskanäle zu entwickeln und schrittweise eine wirksame koordinierte Reaktion auf Unionsebene zu ermöglichen, sofern es zu einem schwerwiegenden grenzüberschreitenden IKT-bezogenen Vorfall oder einer vergleichbaren Bedrohung kommt, die systemische Auswirkungen auf den gesamten Finanzsektor der Union mit sich bringen.

Mit diesen Übungen können gegebenenfalls auch Abhängigkeiten des Finanzsektors von anderen Wirtschaftssektoren untersucht werden.

(2) Die zuständigen Behörden, die ESA und die EZB arbeiten eng zusammen und tauschen Informationen aus, um ihren Aufgaben gemäß den Artikeln 47 bis 54 nachzukommen. Dabei stimmen sie ihre Beaufsichtigungstätigkeit eng untereinander ab, um Verstöße gegen diese Verordnung festzustellen und ihnen entgegenzuwirken, bewährte Verfahren zu entwickeln und zu fördern, die Zusammenarbeit zu erleichtern, eine kohärente Auslegung zu fördern und bei Uneinigkeit eine Bewertung vorzunehmen, die sich nicht nur auf eine einzelne Rechtsordnung stützt.

*Artikel 50*

**Verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen**

(1) Die zuständigen Behörden verfügen über alle Aufsichts-, Untersuchungs- und Sanktionsbefugnisse, die zur Erfüllung ihrer Aufgaben im Rahmen dieser Verordnung erforderlich sind.

(2) Die Befugnisse gemäß Absatz 1 umfassen zumindest folgende Befugnisse:

a) den Zugriff auf Unterlagen oder Daten jeglicher Form, die nach Ansicht der zuständigen Behörde für die Ausführung ihrer Aufgaben von Belang sind, sowie den Erhalt oder Anfertigung von Kopien von ihnen;

b) Durchführung von Vor-Ort-Inspektionen oder Untersuchungen, einschließlich unter anderem

   i) der Vorladung von Vertretern der Finanzunternehmen, damit diese mündliche oder schriftliche Erklärungen zu Sachverhalten oder Unterlagen abgeben, die mit Gegenstand und Zweck der Untersuchung in Zusammenhang stehen, sowie der Aufzeichnung der Antworten,

   ii) der Befragung jeder anderen natürlichen oder juristischen Person, die dieser Befragung zum Zweck der Einholung von Informationen über den Gegenstand einer Untersuchung zustimmt;

c) das Verlangen von Korrektur- und Abhilfemaßnahmen bei Verstößen gegen die Anforderungen dieser Verordnung.

(3) Unbeschadet des Rechts der Mitgliedstaaten, strafrechtliche Sanktionen im Einklang mit Artikel 52 zu verhängen, legen die Mitgliedstaaten angemessene verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen für Verstöße gegen diese Verordnung fest und sorgen für deren wirksame Umsetzung.

Diese Sanktionen und Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein.

(4) Die Mitgliedstaaten übertragen den zuständigen Behörden die Befugnis, bei Verstößen gegen diese Verordnung mindestens die folgenden verwaltungsrechtlichen Sanktionen bzw. Abhilfemaßnahmen anzuwenden:

a) die Erteilung einer Anweisung, wonach die natürliche oder juristische Person gegen diese Verordnung verstoßendes Verhalten zu unterlassen und von einer Wiederholung abzusehen hat;

b) das Verlangen, dass Praktiken oder Verhaltensweisen, die nach Ansicht der zuständigen Behörde den Bestimmungen dieser Verordnung zuwiderlaufen, vorübergehend oder dauerhaft eingestellt und nicht wiederholt werden;

c) das Ergreifen jeder Art von Maßnahme, auch finanzieller Art, um sicherzustellen, dass Finanzunternehmen weiterhin die rechtlichen Anforderungen erfüllen;

d) das Verlangen — soweit gemäß nationalem Recht zulässig — bereits existierender Aufzeichnungen von Datenübermittlungen im Besitz einer Telekommunikationsgesellschaft, wenn der begründete Verdacht auf einen Verstoß gegen die Verordnung besteht und diese Aufzeichnungen für eine Untersuchung von Verstößen gegen diese Verordnung relevant sein könnten; und

e) die Abgabe öffentlicher Bekanntmachungen, einschließlich öffentlicher Bekanntgaben, in denen die Identität der natürlichen oder juristischen Person und die Art des Verstoßes angegeben sind.

(5) Gelten Absatz 2 Buchstabe c und Absatz 4 für juristische Personen, so statten die Mitgliedstaaten die zuständigen Behörden mit der Befugnis aus, Mitgliedern des Leitungsorgans sowie anderen natürlichen Personen, die nach nationalem Recht für den Verstoß verantwortlich sind, vorbehaltlich der nach nationalem Recht geltenden Bedingungen verwaltungsrechtliche Sanktionen und Abhilfemaßnahmen aufzuerlegen.

(6) Die Mitgliedstaaten stellen sicher, dass alle Entscheidungen zur Auferlegung der in Absatz 2 Buchstabe c festgelegten verwaltungsrechtlichen Sanktionen oder Abhilfemaßnahmen ordnungsgemäß begründet werden und dass gegen sie ein Rechtsbehelf eingelegt werden kann.

*Artikel 51*

**Ausübung der Befugnis zur Auferlegung von verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen**

(1) Die zuständigen Behörden üben die Befugnisse zur Auferlegung der in Artikel 50 genannten verwaltungsrechtlichen Sanktionen und Abhilfemaßnahmen innerhalb ihres nationalen Rechtsrahmens je nach Sachlage in folgender Weise aus:

a) direkt;

b) in Zusammenarbeit mit anderen Behörden;

c) unter ihrer Verantwortung durch Übertragung an andere Behörden oder

d) durch Antragstellung bei den zuständigen Justizbehörden.

(2) Bei der Festlegung von Art und Umfang einer nach Artikel 50 auferlegten verwaltungsrechtlichen Sanktion oder Abhilfemaßnahme berücksichtigen die zuständigen Behörden, inwieweit der Verstoß vorsätzlich erfolgte oder das Ergebnis von Fahrlässigkeit ist, sowie alle anderen relevanten Umstände, darunter auch je nach Sachlage:

a) die Wesentlichkeit, Schwere und Dauer des Verstoßes;

b) der Grad an Verantwortung der für den Verstoß verantwortlichen natürlichen oder juristischen Person;

c) die Finanzkraft der verantwortlichen natürlichen oder juristischen Person;

d) die Höhe der von der verantwortlichen natürlichen oder juristischen Person erzielten Gewinne oder verhinderten Verluste, sofern sich diese beziffern lassen;

e) die Verluste, die Dritten durch den Verstoß entstanden sind, sofern sich diese beziffern lassen;

f) die Bereitschaft der verantwortlichen natürlichen oder juristischen Person zur Zusammenarbeit mit der zuständigen Behörde, unbeschadet des Erfordernisses, die von dieser natürlichen oder juristischen Person erzielten Gewinne oder verhinderten Verluste einzuziehen;

g) frühere Verstöße der verantwortlichen natürlichen oder juristischen Person.

*Artikel 52*

**Strafrechtliche Sanktionen**

(1) Mitgliedstaaten können beschließen, für Verstöße, die nach ihrem nationalen Recht strafrechtlichen Sanktionen unterliegen, keine Vorschriften für verwaltungsrechtliche Sanktionen oder Abhilfemaßnahmen festzulegen.

(2) Mitgliedstaaten, die strafrechtliche Sanktionen für die in dieser Verordnung genannten Verstöße festgelegt haben, stellen durch angemessene Maßnahmen sicher, dass die zuständigen Behörden über alle notwendigen Befugnisse verfügen, um sich mit den Justiz-, Strafverfolgungs- oder Strafjustizbehörden in ihrem Hoheitsgebiet ins Benehmen zu setzen, um spezifische Informationen im Zusammenhang mit strafrechtlichen Ermittlungen oder Verfahren, die wegen der Verstöße gegen diese Verordnung eingeleitet wurden, zu erhalten und diese anderen zuständigen Behörden sowie der EBA, der ESMA oder der EIOPA zur Verfügung zu stellen, um ihre Pflichten zur Zusammenarbeit für die Zwecke dieser Verordnung zu erfüllen.

*Artikel 53*

**Mitteilungspflichten**

Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA bis zum 17. Januar 2025 die Gesetze, sonstige Vorschriften sowie Verwaltungsvorschriften, einschließlich der einschlägigen strafrechtlichen Vorschriften, zur Umsetzung dieses Kapitels mit. Die Mitgliedstaaten teilen der Kommission, der ESMA, der EBA und der EIOPA spätere Änderungen dieser Vorschriften unverzüglich mit.

*Artikel 54*

**Öffentliche Bekanntmachung verwaltungsrechtlicher Sanktionen**

(1) Die zuständigen Behörden veröffentlichen auf ihren amtlichen Websites unverzüglich jede Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion, gegen die nach Mitteilung dieser Entscheidung an die Person, gegen die die Sanktion verhängt wurde, kein Rechtsbehelf eingelegt werden kann.

(2) Die in Absatz 1 genannte Bekanntmachung umfasst Informationen zu Art und Natur des Verstoßes, der Identität der verantwortlichen Personen und der verhängten Sanktionen.

(3) Gelangt die zuständige Behörde nach einer Einzelfallprüfung zu der Auffassung, dass die Bekanntmachung der Identität im Falle juristischer Personen oder der Identität und der personenbezogenen Daten im Falle natürlicher Personen unverhältnismäßig wäre, was auch Risiken für den Schutz personenbezogener Daten einschließt, die Stabilität der Finanzmärkte oder die Durchführung laufender strafrechtlicher Ermittlungen gefährden oder der betroffenen Person einen unverhältnismäßigen Schaden zufügen würde — soweit dieser ermittelt werden kann —, so beschließt sie in Bezug auf die Entscheidung, mit der eine verwaltungsrechtliche Sanktion verhängt wird, eine der folgenden Lösungen:

a) Aufschub der Veröffentlichung bis alle Gründe für die Nichtveröffentlichung wegfallen;

b) anonyme Veröffentlichung im Einklang mit dem nationalen Recht; oder

c) Unterlassung der Veröffentlichung, wenn die unter den Buchstaben a und b genannten Optionen entweder nicht ausreichen, um zu gewährleisten, dass keine Gefahr für die Stabilität der Finanzmärkte besteht, oder wenn eine solche Veröffentlichung nicht mit der bei der Verhängung der Sanktion angewandten Nachsicht vereinbar wäre.

(4) Wird entschieden, eine verwaltungsrechtliche Sanktion gemäß Absatz 3 Buchstabe b in anonymisierter Form bekannt zu machen, so kann die Bekanntmachung der einschlägigen Angaben aufgeschoben werden.

(5) Macht eine zuständige Behörde eine Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion, gegen die ein Rechtsbehelf bei den einschlägigen Justizbehörden eingelegt worden ist, bekannt, so fügen die zuständigen Behörden diese Information ihrer amtlichen Website unverzüglich und etwaige nachfolgende Informationen über den Ausgang des Rechtsbehelfsverfahrens zu einem späteren Zeitpunkt hinzu. Gerichtliche Entscheidungen, mit denen eine Entscheidung zur Verhängung einer verwaltungsrechtlichen Sanktion für nichtig erklärt wird, werden ebenfalls bekannt gemacht.

(6) Die zuständigen Behörden stellen sicher, dass die in den Absätzen 1 bis 4 genannten Bekanntmachungen nur so lange auf ihrer amtlichen Website verbleiben, wie es zum Zwecke dieses Artikels erforderlich ist. Dieser Zeitraum darf fünf Jahre ab dem Zeitpunkt der Veröffentlichung nicht überschreiten.

*Artikel 55*

**Wahrung des Berufsgeheimnisses**

(1) Vertrauliche Informationen, die gemäß dieser Verordnung empfangen, ausgetauscht oder übermittelt werden, unterliegen den in Absatz 2 festgelegten Bestimmungen zum Berufsgeheimnis.

(2) Zur Wahrung des Berufsgeheimnisses verpflichtet sind alle Personen, die bei den gemäß dieser Verordnung zuständigen Behörden oder bei einer Behörde, einem Marktteilnehmer oder einer natürlichen oder juristischen Person beschäftigt sind oder waren, an die bzw. den diese zuständigen Behörden ihre Befugnisse delegiert haben, einschließlich unter Vertrag genommener Revisoren und Sachverständigen.

(3) Unter das Berufsgeheimnis fallende Informationen, einschließlich der zwischen den gemäß der vorliegenden Verordnung zuständigen Behörden und den gemäß der Richtlinie (EU) 2022/2555 benannten oder eingerichteten zuständigen Behörden ausgetauschten Informationen, dürfen keiner anderen Person oder Behörde gegenüber offengelegt werden, es sei denn, dies geschieht aufgrund von Unionsrecht oder nationalem Recht.

(4) Alle gemäß dieser Verordnung zwischen den zuständigen Behörden ausgetauschten Informationen, die Geschäfts- oder Betriebsbedingungen und andere wirtschaftliche oder persönliche Angelegenheiten betreffen, werden als vertraulich betrachtet und unterliegen den Anforderungen an das Berufsgeheimnis, es sein denn, ihre Weitergabe wird von der zuständigen Behörde zum Zeitpunkt der Mitteilung für zulässig erklärt oder ist für Gerichtsverfahren erforderlich.

*Artikel 56*

**Datenschutz**

(1) Die ESA und die zuständigen Behörden dürfen personenbezogene Daten nur verarbeiten, wenn dies zur Erfüllung ihrer jeweiligen Pflichten und Aufgaben gemäß dieser Verordnung erforderlich ist, insbesondere für Untersuchungen, Inspektionen, Auskunftsersuchen, Kommunikationszwecke, Veröffentlichungen, Evaluierungen, Verifizierungen, Bewertungen und die Erstellung von Überwachungsplänen. Die personenbezogenen Daten müssen im Einklang mit der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 verarbeitet werden, je nachdem, welche der beiden anwendbar ist.

(2) Sofern in anderen sektorspezifischen Rechtsakten nichts anderes vorgesehen ist, werden die in Absatz 1 genannten personenbezogenen Daten bis zur Erfüllung der geltenden Aufsichtspflichten, in jedem Fall aber für höchstens 15 Jahre aufbewahrt, außer bei anhängigen Gerichtsverfahren, die eine weitere Speicherung dieser Daten erfordern.

*KAPITEL VIII*

***Delegierte Rechtsakte***

*Artikel 57*

**Ausübung der Befugnisübertragung**

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 17. Januar 2024 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 31 Absatz 6 und Artikel 43 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von drei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um drei Monate verlängert.

*KAPITEL IX*

***Übergangs- und Schlussbestimmungen***

Abschnitt I

*Artikel 58*

**Überprüfungsklausel**

(1) Bis zum 17. Januar 2028 führt die Kommission nach Konsultation der ESA und des ESRB, je nach Sachlage, eine Überprüfung durch und legt dem Europäischen Parlament und dem Rat einen Bericht vor, gegebenenfalls zusammen mit einem Gesetzgebungsvorschlag. Die Überprüfung muss sich mindestens auf Folgendes erstrecken:

a) die Kriterien für die Benennung kritischer IKT-Drittdienstleister gemäß Artikel 31 Absatz 2;

b) die Freiwilligkeit der Meldung erheblicher Cyberbedrohungen gemäß Artikel 19;

c) die Regelung gemäß Artikel 31 Absatz 12 und die Befugnisse der federführenden Überwachungsbehörde gemäß Artikel 35 Absatz 1 Buchstabe d Ziffer iv erster Gedankenstrich, um die Wirksamkeit dieser Bestimmungen im Hinblick auf die Gewährleistung einer wirksamen Überwachung kritischer IKT-Drittdienstleister mit Sitz in einem Drittland und die Notwendigkeit der Gründung eines Tochterunternehmens in der Union zu bewerten.

   Für die Zwecke von Unterabsatz 1 dieses Buchstabens umfasst die Überprüfung eine Analyse der Regelung gemäß Artikel 31 Absatz 12, einschließlich hinsichtlich der Bedingungen für den Zugang von Finanzunternehmen der Union zu Dienstleistungen aus Drittländern und der Verfügbarkeit dieser Dienstleistungen auf dem Unionsmarkt, und berücksichtigt weitere Entwicklungen auf den Märkten für die unter diese Verordnung fallenden Dienstleistungen, die von Finanzunternehmen und Finanzaufsichtsbehörden bei der Anwendung dieser Regelung bzw. der damit verbundenen Beaufsichtigung gewonnenen praktischen Erfahrungen sowie alle einschlägigen regulatorischen und aufsichtlichen Entwicklungen auf internationaler Ebene.

d) die Angemessenheit der Einbeziehung derjenigen in Artikel 2 Absatz 3 Buchstabe e genannten Finanzunternehmen in den Geltungsbereich dieser Verordnung, die automatisierte Vertriebssysteme nutzen, unter Berücksichtigung künftiger Marktentwicklungen im Zusammenhang mit der Nutzung solcher Systeme;

e) die Funktionsweise und Wirksamkeit des JON bei der Förderung der Kohärenz der Überwachung und der Effizienz des Informationsaustauschs innerhalb des Überwachungsrahmens.

(2) Im Zusammenhang mit der Überprüfung der Richtlinie (EU) 2015/2366 bewertet die Kommission, ob die Resilienz von Zahlungssystemen und Zahlungsabwicklungstätigkeiten gegenüber Cyberangriffen erhöht werden muss und ob es angemessen ist, den Geltungsbereich dieser Verordnung auf Betreiber von Zahlungssystemen und an Zahlungsabwicklungstätigkeiten beteiligte Stellen auszuweiten. Die Kommission legt unter Berücksichtigung des Ergebnisses dieser Bewertung dem Europäischen Parlament und dem Rat im Rahmen der Überprüfung der Richtlinie (EU) 2015/2366 bis spätestens 17. Juli 2023 einen Bericht vor.

Auf der Grundlage dieses Überprüfungsberichts und nach Konsultation der ESA, der EZB und des ESRB kann die Kommission gegebenenfalls als Teil des Gesetzgebungsvorschlags, den sie gemäß Artikel 108 Unterabsatz 2 der Richtlinie (EU) 2015/2366 annehmen kann, einen Vorschlag unterbreiten, mit dem sichergestellt wird, dass alle Betreiber von Zahlungssystemen und alle an Zahlungsabwicklungstätigkeiten beteiligte Stellen einer angemessenen Überwachung unterliegen, wobei der bestehenden Überwachung durch die Zentralbank Rechnung zu tragen ist.

(3) Bis zum 17. Januar 2026 führt die Kommission nach Konsultation der ESA und des Ausschusses der Europäischen Aufsichtsstellen für Abschlussprüfer eine Überprüfung durch und legt — gegebenenfalls zusammen mit einem Gesetzgebungsvorschlag — dem Europäischen Parlament und dem Rat einen Bericht darüber vor, ob strengere Anforderungen an Abschlussprüfer und Prüfungsgesellschaften in Bezug auf die digitale operationale Resilienz angemessen sind, indem Abschlussprüfer und Prüfungsgesellschaften in den Geltungsbereich der vorliegenden Verordnung aufgenommen werden oder die Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates ([39]) geändert wird.

Abschnitt II

## Änderungen

*Artikel 59*

### Änderungen der Verordnung (EG) Nr. 1060/2009

Die Verordnung (EG) Nr. 1060/2009 wird wie folgt geändert:

1. Anhang I Abschnitt A Nummer 4 Unterabsatz 1 erhält folgende Fassung:

„Eine Ratingagentur verfügt über eine solide Verwaltung und Rechnungslegung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

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

2. Anhang III Nummer 12 erhält folgende Fassung:

„12. Die Ratingagentur verstößt gegen Artikel 6 Absatz 2 in Verbindung mit Anhang I Abschnitt A Nummer 4, wenn sie über keine solide Verwaltung und Rechnungslegung, keine internen Kontrollmechanismen, keine effizienten Verfahren für die Risikobewertung oder keine wirksamen Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 verfügt oder wenn sie keine Entscheidungsprozesse oder keine Organisationsstruktur nach Maßgabe jener Nummer schafft oder unterhält.“

*Artikel 60*

### Änderungen der Verordnung (EU) Nr. 648/2012

Die Verordnung (EU) Nr. 648/2012 wird wie folgt geändert:

1. Artikel 26 wird wie folgt geändert:

a) Absatz 3 erhält folgende Fassung:

„(3) Eine CCP muss dauerhaft über eine Organisationsstruktur verfügen, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet. Sie muss angemessene und verhältnismäßige Systeme, Ressourcen und Verfahren einsetzen, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) betrieben werden.

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

([39]) Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates (ABl. L 157 vom 9.6.2006, S. 87).

b) Absatz 6 wird gestrichen;

2. Artikel 34 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Eine CCP hat eine angemessene Geschäftsfortführungsleitlinie sowie einen Notfallwiederherstellungsplan — der eine IKT-Geschäftsfortführungsleitlinie und IKT- Reaktions- und Wiederherstellungspläne umfasst, die nach der Verordnung (EU) 2022/2554 aufgestellt und umgesetzt werden — festzulegen, umzusetzen und zu befolgen, mit dem Ziel eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie eine Erfüllung der Pflichten der CCP zu gewährleisten."

b) Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA nach Anhörung der Mitglieder des ESZB Entwürfe für technische Regulierungsstandards, in denen der Mindestinhalt und die Anforderungen an die Geschäftsfortführungsleitlinie und an den Notfallwiederherstellungsplan, unter Ausschluss der IKT-Geschäftsfortführungsleitlinie und der Pläne für Notfallwiederherstellung, festgelegt werden."

3. Artikel 56 Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) Um die einheitliche Anwendung dieses Artikels zu gewährleisten, erarbeitet die ESMA Entwürfe für technische Regulierungsstandards, in denen die Einzelheiten des in Absatz 1 genannten Antrags auf Registrierung festgelegt werden, mit Ausnahme der Anforderungen im Zusammenhang mit dem IKT-Risikomanagement."

4. Artikel 79 Absätze 1 und 2 erhält folgende Fassung:

„(1) Ein Transaktionsregister ermittelt Quellen operationeller Risiken und minimiert diese Risiken durch die Entwicklung angemessener Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 betrieben werden.

(2) Ein Transaktionsregister hat eine angemessene Geschäftsfortführungsleitlinie und einen Notfallwiederherstellungsplan — einschließlich einer IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungsplänen, die nach der Verordnung (EU) 2022/2554 eingerichtet werden — festzulegen, umzusetzen und zu befolgen, mit dem Ziel, die Aufrechterhaltung der Funktionen des Transaktionsregisters, die rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters zu gewährleisten."

5. Artikel 80 Absatz 1 wird gestrichen;

6. Anhang I Abschnitt II wird wie folgt geändert:

a) Die Buchstaben a und b erhalten folgende Fassung:

„a) Ein Transaktionsregister verstößt gegen Artikel 79 Absatz 1, wenn es nicht die Quellen betrieblicher Risiken ermittelt bzw. diese Risiken nicht durch die Entwicklung angemessener Systeme, Kontrollen und Verfahren, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 betrieben werden, minimiert.

b) Ein Transaktionsregister verstößt gegen Artikel 79 Absatz 2, wenn es nicht eine angemessene Geschäftsfortführungsleitlinie und einen Notfallwiederherstellungsplan, die nach der Verordnung (EU) 2022/2554 eingerichtet werden, festlegt, umsetzt oder aufrechterhält, mit dem Ziel, die Aufrechterhaltung der Funktionen des Transaktionsregisters, die zeitnahe Wiederherstellung des Geschäftsbetriebs sowie die Erfüllung der Pflichten des Transaktionsregisters zu gewährleisten."

b) Buchstabe c wird gestrichen;

7. Anhang III wird wie folgt geändert:

a) Abschnitt II wird wie folgt geändert:

i) Buchstabe c erhält folgende Fassung:

„c) eine Tier 2-CCP verstößt gegen Artikel 26 Absatz 3, wenn sie nicht dauerhaft über eine Organisationsstruktur verfügt, die Kontinuität und ein ordnungsgemäßes Funktionieren im Hinblick auf die Erbringung ihrer Dienstleistungen und Ausübung ihrer Tätigkeiten gewährleistet, oder wenn sie keine angemessenen und geeigneten Systeme, Ressourcen und Verfahren einsetzt, einschließlich IKT-Systemen, die gemäß der Verordnung (EU) 2022/2554 (DORA) betrieben werden;"

ii) Buchstabe f wird gestrichen.

b) in Abschnitt III erhält Buchstabe a folgende Fassung:

„a) eine Tier 2-CCP verstößt gegen Artikel 34 Absatz 1, wenn sie keine angemessene Geschäftsfortführungsleitlinie und keinen Reaktions- und Wiederherstellungsplan, die nach der Verordnung (EU) 2022/2554 eingerichtet werden, festlegt, umsetzt und befolgt, mit dem Ziel, eine Aufrechterhaltung der Funktionen der CCP, eine rechtzeitige Wiederherstellung des Geschäftsbetriebs sowie eine Erfüllung der Pflichten der CCP zu gewährleisten, wobei ein solcher Plan zumindest eine Wiederherstellung aller Transaktionen zum Zeitpunkt der Störung ermöglichen muss, sodass die CCP weiterhin zuverlässig arbeiten und die Abwicklung zum geplanten Termin vornehmen kann;“

*Artikel 61*

**Änderungen der Verordnung (EU) Nr. 909/2014**

Artikel 45 der Verordnung (EU) Nr. 909/2014 wird wie folgt geändert:

1. Absatz 1 erhält folgende Fassung:

„(1) Ein Zentralverwahrer ermittelt Quellen des internen und externen operationellen Risikos und hält deren Auswirkungen durch den Einsatz angemessener IKT-Tools, Verfahren und Strategien, die gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie durch alle anderen relevanten angemessenen Instrumente, Kontrollen und Verfahren für andere Arten operationeller Risiken, auch für alle von ihm betriebenen Wertpapierliefer- und -abrechnungssysteme, so gering wie möglich.

_____

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

2. Absatz 2 wird gestrichen;

3. Absätze 3 und 4 erhalten folgende Fassung:

„(3) Für die von ihm erbrachten Dienstleistungen und jedes von ihm betriebene Wertpapierliefer- und -abrechnungssystem legt ein Zentralverwahrer eine angemessene Geschäftsfortführungsleitlinie sowie einen Notfallwiederherstellungsplan, einschließlich einer IKT-Geschäftsfortführungsleitlinie und IKT-Reaktions- und Wiederherstellungspläne, die gemäß der Verordnung (EU) 2022/2554 eingerichtet werden, fest, die er anwendet und befolgt, um bei Ereignissen, die ein beträchtliches Risiko einer Beeinträchtigung des Geschäftsbetriebs bergen, das Aufrechterhalten der Dienstleistungen, die rasche Wiederherstellung des Geschäftsbetriebs und die Erfüllung seiner Pflichten zu gewährleisten.

(4) Der Plan nach Absatz 3 muss eine Wiederherstellung aller Geschäfte und Positionen der Teilnehmer zum Zeitpunkt der Störung ermöglichen, damit die Teilnehmer eines Zentralverwahrers ihre Tätigkeiten in sicherer Weise fortsetzen und Lieferungen und Abrechnungen zum geplanten Termin vornehmen können; hierzu gehört auch die Vorsorge, dass kritische IT-Systeme nach der Störung wieder in Betrieb genommen werden können, so wie in Artikel 12 Absätze 5 und 7 der Verordnung (EU) 2022/2554 vorgesehen.“

4. Absatz 6 erhält folgende Fassung:

„(6) Ein Zentralverwahrer ermittelt, überwacht und managt die Risiken, die von wichtigen Teilnehmern an den von ihm betriebenen Wertpapierliefer- und -abrechnungssystemen sowie von Dienstleistern und Versorgungsbetrieben, anderen Zentralverwahrern oder anderen Marktinfrastrukturen für seinen Geschäftsbetrieb ausgehen könnten. Er unterrichtet die zuständige Behörde sowie die betreffenden Behörden auf Verlangen über alle solchermaßen ermittelten Risiken. Er unterrichtet die zuständige Behörde sowie die betreffenden Behörden ferner unverzüglich über alle Störfälle infolge dieser Risiken, die nicht im Zusammenhang mit dem IKT-Risiko auftreten.“

5. Absatz 7 Unterabsatz 1 erhält folgende Fassung:

„(7) Die ESMA arbeitet in enger Abstimmung mit den Mitgliedern des ESZB Entwürfe technischer Regulierungsstandards aus, in denen die operationellen Risiken nach den Absätzen 1 und 6 — mit Ausnahme von IKT-Risiken — sowie die Verfahren zur Prüfung, Bewältigung oder Minimierung dieser Risiken einschließlich der Geschäftsfortführungsleitlinien und der Notfallsanierungspläne nach den Absätzen 3 und 4 sowie der Verfahren zu ihrer Beurteilung präzisiert werden.“

*Artikel 62*

**Änderungen der Verordnung (EU) Nr. 600/2014**

Die Verordnung (EU) Nr. 600/2014 wird wie folgt geändert:

1. Artikel 27g wird wie folgt geändert:

   a) Absatz 4 erhält folgende Fassung:

   „(4) Ein APA muss die in der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   _____

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

   b) Absatz 8 Buchstabe c erhält folgende Fassung:

   „c) die konkreten organisatorischen Anforderungen nach den Absätzen 3 und 5."

2. Artikel 27h wird wie folgt geändert:

   a) Absatz 5 erhält folgende Fassung:

   „(5) Ein CTP muss die in der Verordnung (EU) 2022/2554 festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   b) in Absatz 8 erhält Buchstabe e folgende Fassung:

   „e) die konkreten organisatorischen Anforderungen nach Absatz 4."

3. Artikel 27i wird wie folgt geändert:

   a) Absatz 3 erhält folgende Fassung:

   „(3) Ein ARM muss die in der Verordnung (EU) 2022/2554 festgelegten Anforderungen in Bezug auf die Sicherheit von Netzwerk- und Informationssystemen erfüllen."

   b) Absatz 5 Buchstabe b erhält folgende Fassung:

   „b) die konkreten organisatorischen Anforderungen nach den Absätzen 2 und 4."

*Artikel 63*

**Änderungen der Verordnung (EU) 2016/1011**

In Artikel 6 der Verordnung (EU) 2016/1011 wird folgender Absatz angefügt:

„(6) Für kritische Referenzwerte verfügt ein Administrator über eine solide Verwaltung und Rechnungslegung, interne Kontrollmechanismen, effiziente Verfahren für die Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für den Betrieb von IKT-Systemen gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

_____

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

*Artikel 64*

**Inkrafttreten und Anwendung**

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

Sie gilt ab dem 17. Januar 2025.

Diese Verordnung ist in allen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Geschehen zu Straßburg am 14. Dezember 2022.

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

# RICHTLINIEN

## RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

**vom 14. Dezember 2022**

**über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)**

**(Text von Bedeutung für den EWR)**

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

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

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(73) Die Union kann gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe, dem CSIRTs-Netzwerk und EU-CyCLONe ermöglicht und geregelt wird. Solche Übereinkünfte sollten die Interessen der Union wahren und einen angemessenen Datenschutz gewährleisten. Das sollte nicht das Recht der Mitgliedstaaten ausschließen, mit Drittländern bei der Verwaltung von Schwachstellen und von Cybersicherheitsrisiken zusammenzuarbeiten und die Berichterstattung und den allgemeinen Informationsaustausch im Einklang mit dem Recht der Union zu erleichtern.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

**ALLGEMEINE BESTIMMUNGEN**

*Artikel 1*

**Gegenstand**

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

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

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

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

c) Vorschriften und Pflichten zum Austausch von Cybersicherheitsinformationen;

d) Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten.

*Artikel 2*

**Anwendungsbereich**

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

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

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

a) die Dienste erbracht werden von:

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

   ii) Vertrauensdiensteanbietern;

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

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

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

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

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

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung:

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

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

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

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

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

a) Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene;

b) Bildungseinrichtungen, insbesondere wenn sie kritische Forschungstätigkeiten durchführen.

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

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

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

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

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

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

(12) Diese Richtlinie gilt unbeschadet der Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG, der Richtlinien 2011/93/EU ([27]) und 2013/40/EU ([28]) des Europäischen Parlaments und des Rates sowie der Richtlinie (EU) 2022/2557.

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

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

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

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

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

*Artikel 3*

**Wesentliche und wichtige Einrichtungen**

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

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

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

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

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

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

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

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

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

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

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

a) den Namen der Einrichtung,

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

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

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

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

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

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

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

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

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

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

*Artikel 4*

**Sektorspezifische Rechtsakte der Union**

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

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

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

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

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

*Artikel 5*

**Mindestharmonisierung**

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

*Artikel 6*

**Begriffsbestimmungen**

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Netz- und Informationssystem“

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([29]);

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

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

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

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

20. „DNS-Diensteanbieter“ eine Einrichtung, die

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

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

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

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

23. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([30]);

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

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

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

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

28. „Online-Marktplatz“ einen digitalen Dienst im Sinne des Artikels 2 Buchstabe n der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates ([31]);

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

KAPITEL II

## KOORDINIERTE RAHMEN FÜR DIE CYBERSICHERHEIT

*Artikel 7*

### Nationale Cybersicherheitsstrategie

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

j) zur Förderung eines aktiven Cyberschutzes.

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

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

*Artikel 8*

**Zuständige Behörden und zentrale Anlaufstellen**

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

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

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

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

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

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

*Artikel 9*

**Nationale Rahmen für das Cyberkrisenmanagement**

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

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

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

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

a) die Ziele der nationalen Vorsorgenmaßnahmen und -tätigkeiten;

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

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

d) die nationalen Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen;

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

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

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

*Artikel 10*

**Computer-Notfallteams (CSIRTs)**

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

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

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

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

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

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

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

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

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

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

*Artikel 11*

**Anforderungen an die CSIRTs sowie technische Kapazitäten und Aufgaben der CSIRTs**

(1) Die CSIRTs müssen den folgenden Anforderungen genügen:

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

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

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

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

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

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

Die CSIRTs können sich an internationalen Kooperationsnetzen beteiligen.

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

(3) Die CSIRTs haben folgende Aufgaben:

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

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

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

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

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

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

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

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

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

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

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

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

a) Verfahren zur Bewältigung von Sicherheitsvorfällen,

b) das Krisenmanagement und

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

*Artikel 12*

**Koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank**

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

a) betreffende Einrichtungen zu ermitteln und zu kontaktieren,

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

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

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

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

a) Informationen zur Beschreibung der Schwachstelle,

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

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

*Artikel 13*

**Zusammenarbeit auf nationaler Ebene**

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

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

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

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

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

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

KAPITEL III

**ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE**

*Artikel 14*

**Kooperationsgruppe**

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

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

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

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

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(4) Die Kooperationsgruppe hat folgende Aufgaben:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Artikel 15*

**CSIRTs-Netzwerk**

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

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

(3) Das CSIRTs-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Kapazitäten der CSIRTs;

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

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

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

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

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

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

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

i) Zusammenarbeit, Austausch bewährter Verfahren und Unterstützung der gemäß Artikel 12 Absatz 1 als Koordinatoren benannten CSIRTs im Hinblick auf die Steuerung der koordinierten Offenlegung von Schwachstellen, die erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten nach sich ziehen könnten;

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

   i) Kategorien von Cyberbedrohungen und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

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

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

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

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

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

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

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

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

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

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

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

*Artikel 16*

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

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

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

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

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

(3) Das EU-CyCLONe hat folgende Aufgaben:

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

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

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

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

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

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

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

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

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

*Artikel 17*

**Internationale Zusammenarbeit**

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

*Artikel 18*

**Bericht über den Stand der Cybersicherheit in der Union**

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

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

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

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

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

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

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

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

*Artikel 19*

**Peer Reviews**

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

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

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

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

c) die operativen Kapazitäten der CSIRTs;

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

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

f) spezifische Fragen mit grenz- oder sektorenübergreifendem Charakter.

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

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

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

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

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

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

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

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

## KAPITEL IV

## RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT

### *Artikel 20*

### Governance

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

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

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

*Artikel 21*

**Risikomanagementmaßnahmen im Bereich der Cybersicherheit**

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

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

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

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

b) Bewältigung von Sicherheitsvorfällen;

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

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

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

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

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

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

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

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

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

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

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

Die Kommission kann Durchführungsrechtsakte erlassen, in denen die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen in Bezug auf andere als die in Unterabsatz 1 des vorliegenden Absatzes genannten wesentlichen und wichtigen Einrichtungen festgelegt werden.

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

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

*Artikel 22*

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

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

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

*Artikel 23*

**Berichtspflichten**

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

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

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

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

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

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

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

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

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

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

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

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

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

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

   iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

   iv) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;

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

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

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

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

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

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

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

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

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

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

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

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

*Artikel 24*

**Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung**

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

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

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

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

*Artikel 25*

**Normung**

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

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

KAPITEL V

**ZUSTÄNDIGKEIT UND REGISTRIERUNG**

*Artikel 26*

**Zuständigkeit und Territorialität**

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

a) Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie ihre Dienste erbringen;

b) DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie gemäß Absatz 2 ihre Hauptniederlassung in der Union haben;

c) Einrichtungen der öffentlichen Verwaltung, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, der sie gegründet hat.

(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union einer in Absatz 1 Buchstabe b genannten Einrichtung jeweils die Niederlassung in demjenigen Mitgliedstaat betrachtet wird, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden solche Entscheidungen nicht in der Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die Cybersicherheitsmaßnahmen durchgeführt werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Union hat.

(3) Hat eine in Absatz 1 Buchstabe b genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienste innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es wird davon ausgegangen, dass eine solche Einrichtung der Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Absatzes benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Richtlinie einleiten.

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

(5) Mitgliedstaaten, die ein Rechtshilfeersuchen zu einer in Absatz 1 Buchstabe b genannten Einrichtung erhalten haben, können innerhalb der Grenzen dieses Ersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die betreffende Einrichtung ergreifen, die in ihrem Hoheitsgebiet Dienste anbietet oder ein Netz- und Informationssystem betreibt.

*Artikel 27*

**Register der Einrichtungen**

(1) Die ENISA erstellt und pflegt ein Register der DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke auf der Grundlage der Informationen, die sie von den zentralen Anlaufstellen im Einklang mit Artikel 4 erhalten hat. Auf Ersuchen ermöglicht die ENISA den zuständigen Behörden den Zugang zu diesem Register, wobei sie gegebenenfalls für den Schutz der Vertraulichkeit der Informationen sorgt.

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

a) Name der Einrichtung,

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

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

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

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

f) die IP-Adressbereiche der Einrichtung.

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

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

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

*Artikel 28*

**Datenbank der Domänennamen-Registrierungsdaten**

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

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

a) den Domänennamen;

b) das Datum der Registrierung;

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

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

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

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

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

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

KAPITEL VI

## INFORMATIONSAUSTAUSCH

*Artikel 29*

### Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

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

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

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

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

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

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

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

*Artikel 30*

**Freiwillige Meldung relevanter Informationen**

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

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

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

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

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

KAPITEL VII

**AUFSICHT UND DURCHSETZUNG**

*Artikel 31*

**Allgemeine Aspekte der Aufsicht und Durchsetzung**

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

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

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

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

*Artikel 32*

**Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   i) wiederholte Verstöße,

   ii) eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen,

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

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

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

b) die Dauer des Verstoßes;

c) einschlägige frühere Verstöße der betreffenden Einrichtung;

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

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

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

g) Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;

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

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

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

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

*Artikel 33*

**Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wichtige Einrichtungen**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Artikel 34*

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

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

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

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

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

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

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

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

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

*Artikel 35*

**Verstöße mit Verletzungen des Schutzes personenbezogener Daten**

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

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

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

*Artikel 36*

**Sanktionen**

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

*Artikel 37*

**Amtshilfe**

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

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

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

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

Die in Unterabsatz 1 Buchstabe c genannte Amtshilfe kann Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen. Die ersuchte zuständige Behörde darf das Amtshilfeersuchen nur ablehnen, wenn festgestellt wird, dass sie für die erbetene Amtshilfe nicht zuständig ist, dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde steht oder dass das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, deren Offenlegung bzw. Ausführung den wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung des betreffenden Mitgliedstaats zuwiderlaufen würde. Bevor die zuständige Behörde einen solchen Antrag ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden sowie — auf Ersuchen eines der betreffenden Mitgliedstaaten — die Kommission und die ENISA.

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

KAPITEL VIII

**DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE**

*Artikel 38*

**Ausübung der Befugnisübertragung**

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 24 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 16. Januar 2023 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 24 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 24 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

*Artikel 39*

**Ausschussverfahren**

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

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

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

KAPITEL IX

**SCHLUSSBESTIMMUNGEN**

*Artikel 40*

**Überprüfung**

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

*Artikel 41*

**Umsetzung**

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

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

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

*Artikel 42*

**Änderung der Verordnung (EU) Nr. 910/2014**

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

*Artikel 43*

**Änderung der Richtlinie (EU) 2018/1972**

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

*Artikel 44*

**Aufhebung**

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

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

*Artikel 45*

**Inkrafttreten**

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

*Artikel 46*

**Adressaten**

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 14. Dezember 2022.

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

*ANHANG I*

**SEKTOREN MIT HOHER KRITIKALITÄT**

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

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| 2. Verkehr | a) Luftverkehr | — Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden |
| | | — Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ([6]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates ([7]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben |
| | | — Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates ([8]) bereitstellen |
| | b) Schienenverkehr | — Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ([9]) |
| | | — Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 jener Richtlinie |
| | c) Schifffahrt | — Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates ([10]) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe |
| | | — Leitungsorgane von Häfen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates ([11]), einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben |
| | | — Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates ([12]) |
| | d) Straßenverkehr | — Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ([13]), die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist |
| | | — Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates ([14]) |
| 3. Bankwesen | | Kreditinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates ([15]) |
| 4. Finanzmarktinfrastrukturen | | — Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates ([16]) |
| | | — zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates ([17]) |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| 5. Gesundheitswesen | | — Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([18]) |
| | | — EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates ([19]) |
| | | — Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates ([20]) ausüben<br>— Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen<br>— Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates ([21]) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden |
| 6. Trinkwasser | | Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates ([22]), jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist |
| 7. Abwasser | | Unternehmen, die kommunales Abwasser, häusliches Abwasser oder industrielles Abwasser im Sinne des Artikels 2 Nummern 1, 2 und 3 der Richtlinie 91/271/EWG des Rates ([23]) sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist |
| 8. Digitale Infrastruktur | | — Betreiber von Internet-Knoten |
| | | — DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern |
| | | — TLD-Namenregister |
| | | — Anbieter von Cloud-Computing-Diensten |
| | | — Anbieter von Rechenzentrumsdiensten |
| | | — Betreiber von Inhaltszustellnetzen |
| | | — Vertrauensdiensteanbieter |
| | | — Anbieter öffentlicher elektronischer Kommunikationsnetze oder |
| | | — Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste |
| 9. Verwaltung von IKT-Diensten (Business-to-Business) | | — Anbieter verwalteter Dienste<br>— Anbieter verwalteter Sicherheitsdienste |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| 10. öffentliche Verwaltung | | — Einrichtungen der öffentlichen Verwaltung von Zentralregierungen entsprechend der Definition eines Mitgliedstaats gemäß nationalem Recht |
| | | — Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene entsprechend der Definition eines Mitgliedstaats gemäß nationalem Recht |
| 11. Weltraum | | Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze |

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

([19]) Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26).

([20]) Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates vom 6. November 2001 zur Schaffung eines Gemeinschaftskodexes für Humanarzneimittel (ABl. L 311 vom 28.11.2001, S. 67).

([21]) Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1).

([22]) Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 435 vom 23.12.2020, S. 1).

([23]) Richtlinie 91/271/EWG des Rates vom 21. Mai 1991 über die Behandlung von kommunalem Abwasser (ABl. L 135 vom 30.5.1991, S. 40).

*ANHANG II*

**SONSTIGE KRITISCHE SEKTOREN**

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| 1. Post- und Kurierdienste | | Anbieter von Postdiensten im Sinne des Artikels 2 Nummer 1a der Richtlinie 97/67/EG, einschließlich Anbieter von Kurierdiensten |
| 2. Abfallbewirtschaftung | | Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates ([1]), ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist |
| 3. Produktion, Herstellung und Handel mit chemischen Stoffen | | Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates ([2]), die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren |
| 4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln | | Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates ([3]), die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind |
| 5. Verarbeitendes Gewerbe/Herstellung von Waren | a) Herstellung von Medizinprodukten und In-vitro-Diagnostika | Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates ([4]) herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates ([5]) herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen |
| | b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen | Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben |
| | c) Herstellung von elektrischen Ausrüstungen | Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben |
| | d) Maschinenbau | Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben |
| | e) Herstellung von Kraftwagen und Kraftwagenteilen | Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben |
| | f) sonstiger Fahrzeugbau | Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben |

| Sektor | Teilsektor | Art der Einrichtung |
|---|---|---|
| 6. Anbieter digitaler Dienste | | — Anbieter von Online-Marktplätzen |
| | | — Anbieter von Online-Suchmaschinen |
| | | — Anbieter von Plattformen für Dienste sozialer Netzwerke |
| 7. Forschung | | Forschungseinrichtungen |

([1]) Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über Abfälle und zur Aufhebung bestimmter Richtlinien (ABl. L 312 vom 22.11.2008, S. 3).

([2]) Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Chemikalienagentur, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission (ABl. L 396 vom 30.12.2006, S. 1).

([3]) Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1).

([4]) Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1).

([5]) Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176).

*ANHANG III*

**ENTSPRECHUNGSTABELLE**

| Richtlinie (EU) 2016/1148 | Vorliegende Richtlinie |
|---|---|
| Artikel 1 Absatz 1 | Artikel 1 Absatz 1 |
| Artikel 1 Absatz 2 | Artikel 1 Absatz 2 |
| Artikel 1 Absatz 3 | — |
| Artikel 1 Absatz 4 | Artikel 2 Absatz 12 |
| Artikel 1 Absatz 5 | Artikel 2 Absatz 13 |
| Artikel 1 Absatz 6 | Artikel 2 Absätze 6 und 11 |
| Artikel 1 Absatz 7 | Artikel 4 |
| Artikel 2 | Artikel 2 Absatz 14 |
| Artikel 3 | Artikel 5 |
| Artikel 4 | Artikel 6 |
| Artikel 5 | — |
| Artikel 6 | — |
| Artikel 7 Absatz 1 | Artikel 7 Absätze 1 und 2 |
| Artikel 7 Absatz 2 | Artikel 7 Absatz 4 |
| Artikel 7 Absatz 3 | Artikel 7 Absatz 3 |
| Artikel 8 Absätze 1 bis 5 | Artikel 8 Absätze 1 bis 5 |
| Artikel 8 Absatz 6 | Artikel 13 Absatz 4 |
| Artikel 8 Absatz 7 | Artikel 8 Absatz 6 |
| Artikel 9 Absätze 1, 2 und 3 | Artikel 10 Absätze 1, 2 und 3 |
| Artikel 9 Absatz 4 | Artikel 10 Absatz 9 |
| Artikel 9 Absatz 5 | Artikel 10 Absatz 10 |
| Artikel 10 Absätze 1 und 2 und Absatz 3 Unterabsatz 1 | Artikel 13 Absätze 1, 2 und 3 |
| Artikel 10 Absatz 3 Unterabsatz 2 | Artikel 23 Absatz 9 |
| Artikel 11 Absatz 1 | Artikel 14 Absätze 1 und 2 |
| Artikel 11 Absatz 2 | Artikel 14 Absatz 3 |
| Artikel 11 Absatz 3 | Artikel 14 Absatz 4 Unterabsatz 1 Buchstaben a bis q und Buchstabe s und Absatz 7 |
| Artikel 11 Absatz 4 | Artikel 14 Absatz 4 Unterabsatz 1 Buchstabe r und Unterabsatz 2 |
| Artikel 11 Absatz 5 | Artikel 14 Absatz 8 |
| Artikel 12 Absätze 1 bis 5 | Artikel 15 Absätze 1 bis 5 |
| Artikel 13 | Artikel 17 |
| Artikel 14 Absätze 1 und 2 | Artikel 21 Absätze 1 bis 4 |
| Artikel 14 Absatz 3 | Artikel 23 Absatz 1 |
| Artikel 14 Absatz 4 | Artikel 23 Absatz 3 |
| Artikel 14 Absatz 5 | Artikel 23 Absätze 5, 6 und 8 |

| Richtlinie (EU) 2016/1148 | Vorliegende Richtlinie |
|---|---|
| Artikel 14 Absatz 6 | Artikel 23 Absatz 7 |
| Artikel 14 Absatz 7 | Artikel 23 Absatz 11 |
| Artikel 15 Absatz 1 | Artikel 31 Absatz 1 |
| Artikel 15 Absatz 2 Unterabsatz 1 Buchstabe a | Artikel 32 Absatz 2 Buchstabe e |
| Artikel 15 Absatz 2 Unterabsatz 1 Buchstabe b | Artikel 32 Absatz 2 Buchstabe g |
| Artikel 15 Absatz 2 Unterabsatz 2 | Artikel 32 Absatz 3 |
| Artikel 15 Absatz 3 | Artikel 32 Absatz 4 Buchstabe b |
| Artikel 15 Absatz 4 | Artikel 31 Absatz 3 |
| Artikel 16 Absätze 1 und 2 | Artikel 21 Absätze 1 bis 4 |
| Artikel 16 Absatz 3 | Artikel 23 Absatz 1 |
| Artikel 16 Absatz 4 | Artikel 23 Absatz 3 |
| Artikel 16 Absatz 5 | — |
| Artikel 16 Absatz 6 | Artikel 23 Absatz 6 |
| Artikel 16 Absatz 7 | Artikel 23 Absatz 7 |
| Artikel 16 Absätze 8 und 9 | Artikel 21 Absatz 5 und Artikel 23 Absatz 11 |
| Artikel 16 Absatz 10 | — |
| Artikel 16 Absatz 11 | Artikel 2 Absätze 1, 2 und 3 |
| Artikel 17 Absatz 1 | Artikel 33 Absatz 1 |
| Artikel 17 Absatz 2 Buchstabe a | Artikel 32 Absatz 2 Buchstabe e |
| Artikel 17 Absatz 2 Buchstabe b | Artikel 32 Absatz 4 Buchstaben b |
| Artikel 17 Absatz 3 | Artikel 37 Absatz 1 Buchstaben a und b |
| Artikel 18 Absatz 1 | Artikel 26 Absatz 1 Buchstabe b und Absatz 2 |
| Artikel 18 Absatz 2 | Artikel 26 Absatz 3 |
| Artikel 18 Absatz 3 | Artikel 26 Absatz 4 |
| Artikel 19 | Artikel 25 |
| Artikel 20 | Artikel 30 |
| Artikel 21 | Artikel 36 |
| Artikel 22 | Artikel 39 |
| Artikel 23 | Artikel 40 |
| Artikel 24 | — |
| Artikel 25 | Artikel 41 |
| Artikel 26 | Artikel 45 |
| Artikel 27 | Artikel 46 |
| Anhang I Nummer 1 | Artikel 11 Absatz 1 |
| Anhang I Nummer 2 Buchstabe a Ziffern i bis iv | Artikel 11 Absatz 2 Buchstaben a bis d |

| Richtlinie (EU) 2016/1148 | Vorliegende Richtlinie |
|---|---|
| Anhang I Nummer 2 Buchstabe a Ziffer v | Artikel 11 Absatz 2 Buchstabe f |
| Anhang I Nummer 2 Buchstabe b | Artikel 11 Absatz 4 |
| Anhang I Nummer 2 Buchstabe c Ziffern i und ii | Artikel 11 Absatz 5 Buchstabe a |
| Anhang II | Anhang I |
| Anhang III Nummern 1 und 2 | Anhang II Nummer 6 |
| Anhang III Nummer 3 | Anhang I Nummer 8 |

# RICHTLINIE (EU) 2022/2556 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

**vom 14. Dezember 2022**

**zur Änderung der Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 hinsichtlich der digitalen operationalen Resilienz im Finanzsektor**

**(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 53 Absatz 1 und Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme der Europäischen Zentralbank ([1]),

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Die Union muss den digitalen Risiken, die sich aus dem verstärkten Einsatz von Informations- und Kommunikationstechnologien (IKT) bei der Bereitstellung und Nutzung von Finanzdienstleistungen ergeben und sämtliche Finanzunternehmen betreffen, angemessen und umfassend begegnen und damit ihren Beitrag zur Realisierung des Potenzials des digitalen Finanzwesens leisten, indem Innovationen vorangetrieben werden und der Wettbewerb in einem sicheren digitalen Umfeld gefördert wird.

(2) Finanzunternehmen sind in ihrem Geschäftsalltag sehr stark auf die Nutzung digitaler Technologien angewiesen. Es ist daher von größter Bedeutung, die operationale Resilienz ihres digitalen Betriebs gegenüber IKT-Risiken sicherzustellen. Dies ist angesichts der Zunahme von bahnbrechenden Technologien am Markt — insbesondere Technologien, die die digitale Darstellung von Werten oder Rechten, die mittels Distributed-Ledger- oder ähnlicher Technologie (Kryptowerte) gespeichert werden, ermöglichen — sowie von Dienstleistungen im Zusammenhang mit Kryptowerten dringender geworden.

([1]) ABl. C 343 vom 26.8.2021, S. 1.
([2]) ABl. C 155 vom 30.4.2021, S. 38.
([3]) Standpunkt des Europäischen Parlaments vom 10. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 28. November 2022.

(3) Auf Unionsebene enthalten derzeit die Richtlinien 2009/65/EG ([4]), 2009/138/EG ([5]), 2011/61/EU ([6]), 2013/36/EU ([7]), 2014/59/EU ([8]), 2014/65/EU ([9]), (EU) 2015/2366 ([10]) und (EU) 2016/2341 ([11]) des Europäischen Parlaments und des Rates die Bestimmungen zum Management von IKT-Risiken im Finanzsektor.

Diese Bestimmungen sind uneinheitlich und stellenweise lückenhaft. Das IKT-Risiko wird in einigen Fällen nur implizit als Teil des operationellen Risikos behandelt, während es in anderen Fällen überhaupt nicht behandelt wird. Diese Probleme werden durch die Annahme der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([12]) behoben. Um die Kohärenz mit der genannten Verordnung zu gewährleisten, sollten die genannten Richtlinien daher geändert werden. Durch die vorliegende Richtlinie werden eine Reihe von Änderungen vorgenommen, die erforderlich sind, um für Rechtsklarheit und Kohärenz bei der durch die gemäß den genannten Richtlinien zugelassenen und beaufsichtigten Finanzunternehmen erfolgende Anwendung von unterschiedlichen Anforderungen an die digitale operationale Resilienz, die für die Ausführung ihrer unternehmerischer Tätigkeiten und für die Erbringung von Dienstleistungen erforderlich sind, zu sorgen, wodurch das reibungslose Funktionieren des Binnenmarkts gewährleistet wird. Es ist erforderlich, dafür zu sorgen, dass diese Anforderungen in Bezug auf die Marktentwicklungen angemessen sind, und zugleich die Verhältnismäßigkeit — insbesondere in Bezug auf die Größe von Finanzunternehmen und die besonderen für sie geltenden Regelungen — mit dem Ziel zu fördern, die Befolgungskosten zu senken.

(4) Im Bereich der Bankdienstleistungen enthält die Richtlinie 2013/36/EU derzeit nur allgemeine interne Governance-Vorschriften und Bestimmungen für operationelle Risiken, einschließlich Anforderungen an Notfallpläne und Geschäftsfortführungspläne, die implizit als Grundlage zum Angehen von IKT-Risiken dienen. Um IKT-Risiken explizit und klar anzugehen, sollten jedoch die Anforderungen an Notfallpläne und Geschäftsfortführungspläne im Einklang mit den Anforderungen der Verordnung (EU) 2022/2554 geändert werden, damit auch Geschäftsfortführungspläne und Reaktions- und Wiederherstellungspläne betreffend IKT-Risiken aufgenommen werden. Ferner werden IKT-Risiken im aufsichtlichen Überprüfungs- und Bewertungsprozess (Supervisory Review and Evaluation Process, SREP), der von den zuständigen Behörden durchgeführt wird, nur als Teil des operationellen Risikos implizit berücksichtigt, und die betreffenden Bewertungskriterien sind derzeit in den von der Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde, EBA) herausgegebenen Leitlinien für die IKT-Risikobewertung im Rahmen des aufsichtlichen Überprüfungs- und Bewertungsprozesses (Supervisory Review and Evaluation process — SREP) festgelegt, die durch die Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates ([13]) eingerichtet wurden. Um Rechtsklarheit zu schaffen und sicherzustellen, dass die Bankenaufsichts-

([4]) Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW) (ABl. L 302 vom 17.11.2009, S. 32).

([5]) Richtlinie 2009/138/EG des Europäischen Parlaments und des Rates vom 25. November 2009 betreffend die Aufnahme und Ausübung der Versicherungs- und der Rückversicherungstätigkeit (Solvabilität II) (ABl. L 335 vom 17.12.2009, S. 1).

([6]) Richtlinie 2011/61/EU des Europäischen Parlaments und des Rates vom 8. Juni 2011 über die Verwalter alternativer Investmentfonds und zur Änderung der Richtlinien 2003/41/EG und 2009/65/EG und der Verordnungen (EG) Nr. 1060/2009 und (EU) Nr. 1095/2010 (ABl. L 174 vom 1.7.2011, S. 1).

([7]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([8]) Richtlinie 2014/59/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 zur Festlegung eines Rahmens für die Sanierung und Abwicklung von Kreditinstituten und Wertpapierfirmen und zur Änderung der Richtlinie 82/891/EWG des Rates, der Richtlinien 2001/24/EG, 2002/47/EG, 2004/25/EG, 2005/56/EG, 2007/36/EG, 2011/35/EU, 2012/30/EU und 2013/36/EU sowie der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates (ABl. L 173 vom 12.6.2014, S. 190).

([9]) 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).

([10]) Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG (ABl. L 337 vom 23.12.2015, S. 35).

([11]) Richtlinie (EU) 2016/2341 des Europäischen Parlaments und des Rates vom 14. Dezember 2016 über die Tätigkeiten und die Beaufsichtigung von Einrichtungen der betrieblichen Altersversorgung (EbAV) (ABl. L 354 vom 23.12.2016, S. 37).

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

([13]) Verordnung (EU) Nr. 1093/2010 des Europäischen Parlaments und des Rates vom 24. November 2010 zur Errichtung einer Europäischen Aufsichtsbehörde (Europäische Bankenaufsichtsbehörde), zur Änderung des Beschlusses Nr. 716/2009/EG und zur Aufhebung des Beschlusses 2009/78/EG der Kommission (ABl. L 331 vom 15.12.2010, S. 12).

behörden die IKT-Risiken gemäß dem neuen Rahmen für digitale operationale Resilienz wirksam ermitteln und deren Management durch Finanzunternehmen überwachen, sollte der Anwendungsbereich des SREP auch dahingehend geändert werden, dass die in der Verordnung (EU) 2022/2554 niedergelegten Vorgaben explizit genannt und insbesondere die Risiken abgedeckt werden, die durch Berichte über schwerwiegende IKT-bezogene Vorfälle und durch die Ergebnisse der von Finanzunternehmen im Einklang mit jener Verordnung durchgeführten Tests der digitalen operationalen Resilienz aufgedeckt werden.

(5) Die digitale operationale Resilienz ist unverzichtbar, um die kritischen Funktionen und Kerngeschäftsbereiche eines Finanzunternehmens im Falle seiner Abwicklung aufrechtzuerhalten und dadurch Störungen der Realwirtschaft und des Finanzsystems zu vermeiden. Größere betriebliche Vorfälle können die Fähigkeit eines Finanzunternehmens, den Betrieb aufrechtzuerhalten, beeinträchtigen und die Abwicklungsziele gefährden. Bestimmte vertragliche Vereinbarungen betreffend die Nutzung von IKT-Dienstleistungen sind unverzichtbar, um die Aufrechterhaltung des Betriebs sicherzustellen und im Falle der Abwicklung die erforderlichen Daten bereitzustellen. Um die Richtlinie 2014/59/EU mit den Zielen des Unionsrahmens für die operationale Resilienz in Einklang zu bringen, sollte sie entsprechend geändert werden, damit sichergestellt ist, dass Informationen über die operationale Resilienz im Zusammenhang mit der Abwicklungsplanung und der Bewertung der Abwicklungsfähigkeit von Finanzunternehmen berücksichtigt werden.

(6) Nach der Richtlinie 2014/65/EU gelten strengere IKT-Risikovorschriften für Wertpapierfirmen und Handelsplätze, die algorithmischen Handel betreiben. Weniger detaillierte Vorschriften gelten für Datenbereitstellungsdienstleistungen und Transaktionsregister. Außerdem enthält die Richtlinie 2014/65/EU nur wenige Verweise auf Kontroll- und Sicherungsvorkehrungen für Informationsverarbeitungssysteme sowie auf die Nutzung geeigneter Systeme, Ressourcen und Verfahren, um die Kontinuität und Ordnungsmäßigkeit von Dienstleistungen zu gewährleisten. Des Weiteren sollte die genannte Richtlinie in Bezug auf Kontinuität und Ordnungsmäßigkeit bei der Erbringung von Wertpapierdienstleistungen sowie bei der Ausübung von Anlagetätigkeiten, der operationalen Resilienz, der Kapazität von Handelssystemen sowie der Wirksamkeit der Vorkehrungen zur Fortführung der Geschäftstätigkeit und des Risikomanagements mit der Verordnung (EU) 2022/2554 in Einklang gebracht werden.

(7) Die Richtlinie (EU) 2015/2366 enthält spezifische Vorschriften für IKT-Sicherheitskontrollen und Risikominderungsmaßnahmen für die Zwecke der Erteilung einer Zulassung für die Erbringung von Zahlungsdiensten. Diese Zulassungsvorschriften sollten geändert werden, um sie an die Verordnung (EU) 2022/2554 anzugleichen. Darüber hinaus sollten zur Verringerung des Verwaltungsaufwands und zur Vermeidung von Komplexität und doppelten Meldepflichten die Vorschriften für die Meldung von Sicherheitsvorfällen gemäß der Richtlinie (EU) 2015/2366 keine Anwendung auf Zahlungsdienstleister mehr finden, die jener Richtlinie und der Verordnung (EU) 2022/2554 unterliegen, um ihnen den Vorteil eines einheitlichen und vollständig harmonisierten Mechanismus für die Meldung von Vorfällen in Bezug auf alle betrieblichen Vorfälle oder zahlungsbezogene Sicherheitsvorfälle — unabhängig davon, ob ein IKT-Bezug besteht — zu ermöglichen.

(8) Die Richtlinien 2009/138/EG und (EU) 2016/2341 decken IKT-Risiken teilweise in ihren allgemeinen Bestimmungen über Governance und Risikomanagement ab, wobei bestimmte Anforderungen durch delegierte Rechtsakte mit oder ohne spezifische Verweise auf IKT-Risiken festgelegt werden können. Ebenso gelten für Verwalter alternativer Investmentfonds, die der Richtlinie 2011/61/EU unterliegen, und Verwaltungsgesellschaften, die der Richtlinie 2009/65/EG unterliegen, nur sehr allgemeine Vorschriften. Diese Richtlinien sollten daher an die Anforderungen für die Verwaltung von IKT-Systemen und -Tools der Verordnung (EU) 2022/2554 angeglichen werden.

(9) In vielen Fällen wurden weitere IKT-Risikoanforderungen bereits in delegierten Rechtsakten und Durchführungsrechtsakten festgelegt, die basierend auf von der zuständigen Europäischen Aufsichtsbehörde ausgearbeiteten Entwürfen technischer Regulierungs- und Durchführungsstandards angenommen wurden. Da die Bestimmungen der Verordnung (EU) 2022/2554 künftig den Rechtsrahmen für IKT-Risiken im Finanzsektor bilden, sollten bestimmte Ermächtigungen zum Erlass von delegierten Rechtsakten und Durchführungsrechtsakten in den Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU und 2014/65/EU geändert werden, um die Bestimmungen zu IKT-Risiken vom Geltungsbereich dieser Ermächtigungen auszuschließen.

(10) Um eine kohärente Anwendung des neuen Rahmens für digitale operationale Resilienz im Finanzsektor zu gewährleisten, sollten die Mitgliedstaaten die nationalen Rechtsvorschriften zur Umsetzung der vorliegenden Richtlinie ab dem Geltungsbeginn der Verordnung (EU) 2022/2554 anwenden.

(11) Die Richtlinien 2009/65/EG, 2009/138/EG, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 und (EU) 2016/2341 wurden auf der Grundlage von Artikel 53 Absatz 1 oder Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) oder beiden angenommen. Der Gegenstand und die Ziele der in der vorliegenden Richtlinie enthaltenen Änderungen sind miteinander verflochten und wurden daher in einem einzigen Rechtsakt zusammengefasst. Diese Richtlinie sollte daher auf der Grundlage von Artikel 53 Absatz 1 und Artikel 114 AEUV angenommen werden.

(12) Da die Ziele dieser Richtlinie von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, da sie die Harmonisierung von bereits in Richtlinien enthaltenen Anforderungen beinhalten, sondern vielmehr wegen des Umfangs und der Wirkungen der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im 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 dieser Ziele erforderliche Maß hinaus.

(13) Gemäß der Gemeinsamen Politischen Erklärung der Mitgliedstaaten und der Kommission zu erläuternden Dokumenten ([14]) vom 28. September 2011 haben sich die Mitgliedstaaten verpflichtet, in begründeten Fällen zusätzlich zur Mitteilung ihrer Umsetzungsmaßnahmen ein oder mehrere Dokumente zu übermitteln, in denen der Zusammenhang zwischen den Bestandteilen einer Richtlinie und den entsprechenden Teilen nationaler Umsetzungsinstrumente erläutert wird. Für diese Richtlinie hält der Gesetzgeber die Übermittlung derartiger Dokumente für gerechtfertigt —

HABEN FOLGENDE RICHTLINIE ERLASSEN:

*Artikel 1*

**Änderungen der Richtlinie 2009/65/EG**

Artikel 12 der Richtlinie 2009/65/EG wird wie folgt geändert:

1. Absatz 1 Unterabsatz 2 Buchstabe a erhält folgende Fassung:

„a) über eine ordnungsgemäße Verwaltung und Buchhaltung, Kontroll- und Sicherheitsvorkehrungen für die elektronische Datenverarbeitung, einschließlich in Bezug auf Netzwerk- und Informationssysteme, die im Einklang mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie angemessene interne Kontrollverfahren, zu denen insbesondere Regeln für persönliche Geschäfte ihrer Angestellten und für das Halten oder Verwalten von Anlagen in Finanzinstrumenten zum Zwecke der Anlage auf eigene Rechnung gehören, verfügen muss, durch die zumindest gewährleistet wird, dass jedes den OGAW betreffende Geschäft nach Herkunft, Vertragsparteien, Art, Abschlusszeitpunkt und -ort rekonstruiert werden kann und dass die Vermögenswerte der von der Verwaltungsgesellschaft verwalteten OGAW gemäß den Vertragsbedingungen oder Satzungen dieser Fonds sowie gemäß den geltenden rechtlichen Bestimmungen angelegt wird;

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

2. Absatz 3 erhält folgende Fassung:

„(3) Unbeschadet des Artikels 116 erlässt die Kommission mittels delegierter Rechtsakte nach Artikel 112a Maßnahmen zur Festlegung:

a) der Verfahren und Regelungen gemäß Absatz 1 Unterabsatz 2 Buchstabe a mit Ausnahme der Verfahren und Regelungen bezüglich Netzwerk- und Informationssysteme;

b) der Strukturen und organisatorischen Anforderungen zur Verringerung von Interessenkonflikten gemäß Absatz 1 Unterabsatz 2 Buchstabe b.“

([14]) ABl. C 369 vom 17.12.2011, S. 14.

*Artikel 2*

**Änderungen der Richtlinie 2009/138/EG**

Die Richtlinie 2009/138/EG wird wie folgt geändert:

1. Artikel 41 Absatz 4 erhält folgende Fassung:

„(4) Versicherungs- und Rückversicherungsunternehmen treffen angemessene Vorkehrungen, einschließlich der Entwicklung von Notfallplänen, um die Kontinuität und Ordnungsmäßigkeit ihrer Tätigkeiten zu gewährleisten. Zu diesem Zweck greift das Unternehmen auf geeignete und verhältnismäßige Systeme, Ressourcen und Verfahren zurück, richtet insbesondere Netzwerk- und Informationssysteme ein und verwaltet diese gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

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

2. In Artikel 50 Absatz 1 erhalten die Buchstaben a und b folgende Fassung:

„a) die Bestandteile der in den Artikeln 41, 44, insbesondere die unter Artikel 44 Absatz 2 aufgeführten Bereiche, 46 und 47 genannten Systeme mit Ausnahme derjenigen, die das Risikomanagement im Bereich der Informations- und Kommunikationstechnologie betreffen;

b) die in den Artikeln 44, 46, 47 und 48 genannten Funktionen mit Ausnahme der Funktionen im Zusammenhang mit dem Risikomanagement im Bereich der Informations- und Kommunikationstechnologie.“.

*Artikel 3*

**Änderung der Richtlinie 2011/61/EU**

Artikel 18 der Richtlinie 2011/61/EU erhält folgende Fassung:

„*Artikel 18*

**Allgemeine Grundsätze**

(1) Die Mitgliedstaaten legen fest, dass die AIFM für die ordnungsgemäße Verwaltung der AIF jederzeit angemessene und geeignete personelle und technische Ressourcen einsetzen.

Insbesondere schreiben die zuständigen Behörden des Herkunftsmitgliedstaats des AIFM — auch unter Berücksichtigung der Art der von dem AIFM verwalteten AIF — vor, dass der betreffende AIFM über eine ordnungsgemäße Verwaltung und Buchhaltung, Kontroll- und Sicherheitsvorkehrungen für die elektronische Datenverarbeitung, einschließlich in Bezug auf Netzwerk- und Informationssysteme, die im Einklang mit der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichtet und verwaltet werden, sowie angemessene interne Kontrollverfahren, zu denen insbesondere Regeln für persönliche Geschäfte ihrer Angestellten und für das Halten oder Verwalten von Anlagen zum Zwecke der Anlage auf eigene Rechnung gehören, verfügt, durch die zumindest gewährleistet wird, dass jedes die AIF betreffende Geschäft nach Herkunft, Vertragsparteien, Art, Abschlusszeitpunkt und -ort rekonstruiert werden kann und dass die Vermögenswerte der vom AIFM verwalteten AIF gemäß den Vertragsbedingungen oder Satzungen der AIF sowie gemäß den geltenden rechtlichen Bestimmungen angelegt werden.

(2) Die Kommission erlässt gemäß Artikel 56 und nach Maßgabe der Bedingungen der Artikel 57 und 58 delegierte Rechtsakte, mit denen die Verfahren und Regelungen gemäß Absatz 1 mit Ausnahme der Verfahren und Regelungen bezüglich Netzwerk- und Informationssysteme festgelegt werden.

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

*Artikel 4*

**Änderungen der Richtlinie 2013/36/EU**

Die Richtlinie 2013/36/EU wird wie folgt geändert:

1. Artikel 65 Absatz 3 Buchstabe a Ziffer vi erhält folgende Fassung:

„vi) Dritte, auf die die Unternehmen im Sinne der Ziffern i bis iv Funktionen oder Tätigkeiten ausgelagert haben, einschließlich IKT-Drittdienstleister gemäß Kapitel V der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*),

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

2. Artikel 74 Absatz 1 Unterabsatz 1 erhält folgende Fassung:

„Die Institute verfügen über solide Unternehmensführungsregelungen, wozu eine klare Organisationsstruktur mit genau festgelegten, transparenten und kohärenten Zuständigkeiten, wirksame Verfahren zur Ermittlung, Steuerung, Überwachung und Meldung der tatsächlichen und potenziellen künftigen Risiken, angemessene interne Kontrollmechanismen, einschließlich solider Verwaltungs- und Rechnungslegungsverfahren, Netzwerk- und Informationssysteme, die gemäß der Verordnung (EU) 2022/2554 eingerichtet und verwaltet werden, sowie eine Vergütungspolitik und -praxis, die mit einem soliden und wirksamen Risikomanagement vereinbar und diesem förderlich sind, zählen.“

3. Artikel 85 Absatz 2 erhält folgende Fassung:

„(2) Die zuständigen Behörden stellen sicher, dass die Institute über angemessene Notfall- und Geschäftsfortführungsleitlinien und -pläne verfügen, einschließlich IKT-Geschäftsfortführungsleitlinien und -plänen sowie IKT-Reaktions- und Wiederherstellungsplänen in Bezug auf die von ihnen genutzte Technologie zur Übermittlung von Informationen, und dass diese Pläne gemäß Artikel 11 der Verordnung (EU) 2022/2554 eingerichtet, verwaltet und getestet werden, damit Institute bei einer schwerwiegenden Betriebsunterbrechung geschäftlich tätig bleiben und Verluste in Folge einer solchen Unterbrechung begrenzen können.“

4. In Artikel 97 Absatz 1 wird folgender Buchstabe angefügt:

„d) die Risiken, die bei Tests der digitalen operationalen Resilienz gemäß Kapitel IV der Verordnung (EU) 2022/2554 aufgedeckt werden.“.

*Artikel 5*

**Änderungen der Richtlinie 2014/59/EU**

Die Richtlinie 2014/59/EU wird wie folgt geändert:

1. Artikel 10 wird wie folgt geändert:

a) Absatz 7 Buchstabe c erhält folgende Fassung:

„c) Ausführungen dazu, wie kritische Funktionen und Kerngeschäftsbereiche im erforderlichen Umfang rechtlich und wirtschaftlich von anderen Funktionen getrennt werden könnten, um ihre Fortführung und die digitale operationale Resilienz nach einem Ausfall des Instituts sicherzustellen;“;

b) Absatz 7 Buchstabe q erhält folgende Fassung:

„q) eine Beschreibung der wesentlichen Prozesse und Systeme zur Fortführung des Geschäftsbetriebs des Instituts, einschließlich der Netzwerk- und Informationssysteme im Sinne der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*);

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

c) In Absatz 9 wird folgender Unterabsatz angefügt:

„Gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 überprüft und — soweit erforderlich — aktualisiert die EBA die technischen Regulierungsstandards, um unter anderem den Bestimmungen des Kapitels II der Verordnung (EU) 2022/2554 Rechnung zu tragen."

2. Der Anhang wird wie folgt geändert:

a) Abschnitt A Nummer 16 erhält folgende Fassung:

„16. eine Aufstellung der Regelungen und Maßnahmen, die zur Fortführung des Geschäftsbetriebs des Instituts, einschließlich der gemäß der Verordnung (EU) 2022/2554 eingerichteten und verwalteten Netzwerk- und Informationssysteme, erforderlich sind;";

b) Abschnitt B wird wie folgt geändert:

i) Nummer 14 erhält folgende Fassung:

„14. Angaben zu den Eigentümern der in Nummer 13 genannten Systeme, zu entsprechenden Dienstgütevereinbarungen und zu Software, Systemen oder Lizenzen, einschließlich Zuordnung zu den jeweiligen juristischen Personen, kritischen Operationen und Kerngeschäftsbereichen des Instituts, sowie Angaben zu kritischen IKT-Drittdienstleistern im Sinne des Artikels 3 Nummer 23 der Verordnung (EU) 2022/2554;";

ii) Folgende Nummer wird eingefügt:

„14a. Ergebnisse der von Instituten im Einklang mit der Verordnung (EU) 2022/2554 durchgeführten Tests der digitalen operationalen Resilienz;";

c) Abschnitt C wird wie folgt geändert:

i) Nummer 4 erhält folgende Fassung:

„4. inwieweit die vom Institut geschlossenen Dienstleistungsvereinbarungen, einschließlich vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen, solide und im Fall einer Abwicklung des Instituts in vollem Umfang durchsetzbar sind;";

ii) Folgende Nummer wird eingefügt:

„4a. die digitale operationale Resilienz derjenigen Netzwerk- und Informationssysteme, die die kritischen Funktionen und Kerngeschäftsbereiche des Instituts unterstützen, wobei Berichte über schwerwiegende IKT-bezogene Vorfälle und die Ergebnisse der entsprechend der Verordnung 2022/2554 durchgeführten Tests der digitalen operationalen Resilienz zu berücksichtigen sind;".

*Artikel 6*

**Änderungen der Richtlinie 2014/65/EU**

Die Richtlinie 2014/65/EU wird wie folgt geändert:

1. Artikel 16 wird wie folgt geändert:

a) Absatz 4 erhält folgende Fassung:

„(4) Eine Wertpapierfirma trifft angemessene Vorkehrungen, um die Kontinuität und Regelmäßigkeit der Wertpapierdienstleistungen und Anlagetätigkeiten zu gewährleisten. Zu diesem Zweck greift sie auf geeignete und verhältnismäßige Systeme, einschließlich gemäß Artikel 7 der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*) eingerichteter und verwalteter Systeme der Informations- und Kommunikationstechnologie (IKT), sowie auf geeignete und verhältnismäßige Ressourcen und Verfahren zurück.

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

b) In Absatz 5 erhalten die Unterabsätze 2 und 3 folgende Fassung:

„Eine Wertpapierfirma muss über eine ordnungsgemäße Verwaltung und Buchhaltung, interne Kontrollmechanismen sowie wirksame Verfahren zur Risikobewertung verfügen.

Unbeschadet der Möglichkeit der zuständigen Behörden, Zugang zu Kommunikation im Einklang mit dieser Richtlinie und mit Verordnung (EU) Nr. 600/2014 zu verlangen, muss eine Wertpapierfirma über solide Sicherheitsmechanismen gemäß den Anforderungen der Verordnung (EU) 2022/2554 verfügen, durch die die Sicherheit und Authentifizierung der Informationsübermittlungswege sichergestellt werden, das Risiko der Datenverfälschung und des unberechtigten Zugriffs minimiert und ein Durchsickern von Informationen verhindert wird, so dass die Vertraulichkeit der Daten jederzeit gewährleistet ist."

2. Artikel 17 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Eine Wertpapierfirma, die algorithmischen Handel betreibt, verfügt über wirksame Systeme und Risikokontrollen, die für das von ihr betriebene Geschäft geeignet sind, um sicherzustellen, dass ihre Handelssysteme entsprechend den Anforderungen in Kapitel II der Verordnung (EU) 2022/2554 belastbar sind und über ausreichende Kapazitäten verfügen, angemessenen Handelsschwellen und Handelsobergrenzen unterliegen sowie die Übermittlung von fehlerhaften Aufträgen oder eine Funktionsweise der Systeme vermieden wird, durch die Störungen auf dem Markt verursacht werden könnten bzw. ein Beitrag zu diesen geleistet werden könnte.

Eine solche Wertpapierfirma verfügt außerdem über wirksame Systeme und Risikokontrollen, um sicherzustellen, dass die Handelssysteme nicht für einen Zweck verwendet werden können, der gegen die Verordnung (EU) Nr. 596/2014 oder die Vorschriften des Handelsplatzes verstößt, mit dem sie verbunden ist.

Die Wertpapierfirma verfügt über wirksame Vorkehrungen zur Fortführung der Geschäftstätigkeiten, einschließlich gemäß Artikel 11 der Verordnung (EU) 2022/2554 aufgestellter IKT-Geschäftsfortführungsleitlinie und -plänen sowie IKT-Reaktions- und Wiederherstellungsplänen, um mit jeglichen Störungen in ihren Handelssystemen umzugehen, und stellt sicher, dass ihre Systeme vollständig getestet sind und ordnungsgemäß überwacht werden, damit die in diesem Absatz festgelegten allgemeinen Anforderungen und die in den Kapiteln II und IV der Verordnung (EU) 2022/2554 festgelegten spezifischen Anforderungen erfüllt werden."

b) Absatz 7 Buchstabe a erhält folgende Fassung:

„a) die Einzelheiten der in den Absätzen 1 bis 6 festgelegten konkreten organisatorischen und nicht mit dem IKT-Risikomanagement zusammenhängenden Anforderungen, die Wertpapierfirmen vorzuschreiben sind, die verschiedene Wertpapierdienstleistungen, Anlagetätigkeiten, Nebendienstleistungen oder entsprechende Kombinationen erbringen bzw. ausüben; in den Präzisierungen zu den organisatorischen Anforderungen gemäß Absatz 5 werden besondere Anforderungen für den direkten Marktzugang und für den geförderten Zugang in einer Weise festgelegt, dass sichergestellt ist, dass die beim geförderten Zugang durchgeführten Kontrollen denjenigen, die beim direkten Marktzugang durchgeführt werden, zumindest gleichwertig sind;".

3. Artikel 47 Absatz 1 wird wie folgt geändert:

a) Buchstabe b erhält folgende Fassung:

„b) um angemessen für die Steuerung seiner Risiken, einschließlich der IKT-Risiken gemäß Kapitel II der Verordnung (EU) 2022/2554, ausgestattet zu sein, angemessene Vorkehrungen und Systeme zur Ermittlung von für seinen Betrieb wesentlichen Risiken einrichtet und wirksame Maßnahmen zur Begrenzung dieser Risiken trifft;";

b) Buchstabe c wird gestrichen.

4. Artikel 48 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die Mitgliedstaaten schreiben vor, dass ein geregelter Markt seine operationale Resilienz zentsprechend den in Kapitel II der Verordnung (EU) 2022/2554 festgelegten Anforderungen herstellt und erhält, um sicherzustellen, dass seine Handelssysteme belastbar sind und über ausreichende Kapazitäten für Spitzenvolumina an Aufträgen und Mitteilungen verfügen, in der Lage sind, unter extremen Stressbedingungen auf den Märkten einen ordnungsgemäßen Handel zu gewährleisten, vollständig geprüft sind, um zu gewährleisten, dass diese Bedingungen erfüllt sind, und wirksamen Vorkehrungen zur Fortführung der Geschäftstätigkeiten unterliegen, die IKT-Geschäftsfortführungsleitlinie und -pläne sowie IKT- Reaktions- und Wiederherstellungspläne gemäß Artikel 11 der Verordnung (EU) 2022/2554 einschließen, um im Fall von Störungen in seinen Handelssystemen die Kontinuität seines Geschäftsbetriebs zu gewährleisten."

b) Absatz 6 erhält folgende Fassung:

„(6) Die Mitgliedstaaten setzen voraus, dass ein geregelter Markt über wirksame Systeme, Verfahren und Vorkehrungen verfügt, einschließlich der Anforderung, dass Mitglieder oder Teilnehmer gemäß den in den Kapiteln II und IV der Verordnung (EU) 2022/2554 festgelegten Anforderungen angemessene Tests von Algorithmen durchführen und ein Umfeld schaffen, um diese Tests zu vereinfachen, um sicherzustellen, dass algorithmische Handelssysteme keine marktstörenden Handelsbedingungen auf dem Markt schaffen oder zu solchen beitragen, und um etwaige marktstörende Handelsbedingungen, die sich aus algorithmischen Handelssystemen ergeben, zu kontrollieren, einschließlich Systemen zur Begrenzung des Verhältnisses nicht ausgeführter Handelsaufträge zu Geschäften, die von einem Mitglied oder Teilnehmer in das System eingegeben werden können, mit dem Ziel, das Auftragsaufkommen zu verlangsamen, wenn das Risiko besteht, dass seine Systemkapazität erreicht wird, und die kleinstmögliche Tick-Größe zu begrenzen und durchzusetzen, die auf dem Markt ausgeführt werden kann."

c) Absatz 12 wird wie folgt geändert:

i) Buchstabe a erhält folgende Fassung:

„a) um die Anforderungen festzulegen, die sicherstellen, dass die Handelssysteme eines geregelten Markts belastbar sind und über ausreichende Kapazität verfügen; davon ausgenommen sind die Anforderungen in Bezug auf die digitale operationale Resilienz;";

ii) Buchstabe g erhält folgende Fassung:

„g) um dafür zu sorgen, dass angemessene Tests durchgeführt werden, um sicherzustellen, dass die algorithmischen Handelssysteme, einschließlich hochfrequenter algorithmischer Handelssysteme, keine marktstörenden Handelsbedingungen auf dem Markt schaffen können; davon ausgenommen sind Tests der digitalen operationalen Resilienz.".

*Artikel 7*

**Änderungen der Richtlinie (EU) 2015/2366**

Die Richtlinie (EU) 2015/2366 wird wie folgt geändert:

1. Artikel 3 Buchstabe j erhält folgende Fassung:

„j) Dienste, die von technischen Dienstleistern erbracht werden, die zwar zur Erbringung der Zahlungsdienste beitragen, jedoch zu keiner Zeit in den Besitz der zu transferierenden Geldbeträge gelangen, wie die Verarbeitung und Speicherung von Daten, vertrauensbildende Maßnahmen und Dienste zum Schutz der Privatsphäre, Nachrichten- und Instanzenauthentisierung, Bereitstellung von Informations- und Kommunikationstechnologie (IKT) und Kommunikationsnetzen sowie Bereitstellung und Wartung der für Zahlungsdienste genutzten Endgeräte und Einrichtungen mit Ausnahme von Zahlungsauslösediensten und Kontoinformationsdiensten;".

2. Artikel 5 Absatz 1 erhält folgende Fassung:

a) Unterabsatz 1 wird wie folgt geändert:

i) Buchstabe e erhält folgende Fassung:

„e) eine Beschreibung der Unternehmenssteuerung und der internen Kontrollmechanismen des Antragstellers einschließlich der Verwaltungs-, Risikomanagement- und Rechnungslegungsverfahren sowie Vereinbarungen über die Nutzung von IKT-Diensten gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*), aus der hervorgeht, dass diese Unternehmenssteuerung und interne Kontrollmechanismen verhältnismäßig, angemessen, zuverlässig und ausreichend sind;

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

ii) Buchstabe f erhält folgende Fassung:

„f) eine Beschreibung der vorhandenen Verfahren für Überwachung, Handhabung und Folgemaßnahmen bei Sicherheitsvorfällen und sicherheitsbezogenen Kundenbeschwerden, einschließlich eines Mechanismus für die Meldung von Vorfällen, der die Meldepflichten des Zahlungsinstituts nach Kapitel III der Verordnung (EU) 2022/2554 berücksichtigt;";

iii) Buchstabe h erhält folgende Fassung:

„h) eine Beschreibung der Vorkehrungen zur Fortführung der Geschäftstätigkeiten, einschließlich klarer Angaben der kritischen Vorgänge, wirksamer IKT-Geschäftsfortführungsleitlinie und -plänen, IKT-Reaktions- und Wiederherstellungsplänen sowie eines Verfahrens für regelmäßige Tests der Angemessenheit und Wirksamkeit dieser Pläne gemäß der Verordnung (EU) 2022/2554;";

b) Unterabsatz 3 erhält folgende Fassung:

„Bei den in Unterabsatz 1 Buchstabe j genannten Sicherheitskontroll- und Risikominderungsmaßnahmen ist anzugeben, auf welche Weise dadurch ein hohes Maß an digitaler operationaler Resilienz entsprechend Kapitel II der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates, insbesondere bezüglich technischer Sicherheit und Datenschutz gewährleistet wird; das gilt auch für Software und IKT-Systeme, die der Antragsteller oder die Unternehmen, an die er den Betrieb oder Teile des Betriebs dieser auslagert, verwenden. Zu diesen Maßnahmen gehören auch die Sicherheitsmaßnahmen gemäß Artikel 95 Absatz 1. Bei diesen Maßnahmen ist den in Artikel 95 Absatz 3 genannten Leitlinien für Sicherheitsmaßnahmen der EBA Rechnung zu tragen, sobald diese vorliegen."

3. Artikel 19 Absatz 6 Unterabsatz 2 erhält folgende Fassung:

„Die Auslagerung wichtiger betrieblicher Aufgaben, einschließlich IKT-Systemen, darf nicht auf eine Weise erfolgen, dass die Qualität der internen Kontrolle des Zahlungsinstituts und die Möglichkeit der zuständigen Behörde, zu überprüfen und zurückzuverfolgen, ob das Zahlungsinstitut sämtlichen Anforderungen dieser Richtlinie genügt, wesentlich beeinträchtigt werden."

4. Dem Artikel 95 Absatz 1 wird folgender Unterabsatz angefügt:

„Unterabsatz 1 gilt unbeschadet der Anwendung von Kapitel II der Verordnung (EU) 2022/2554 auf

a) Zahlungsdienstleister im Sinne des Artikels 1 Absatz 1 Buchstaben a, b und d,

b) Kontoinformationsdienstleister im Sinne des Artikels 33 Absatz 1,

c) Zahlungsinstitute, die gemäß Artikel 32 Absatz 1 ausgenommen sind, und

d) E-Geld-Institute, für die eine Ausnahme gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt;".

5. Dem Artikel 96 wird folgender Absatz angefügt:

„(7) Die Mitgliedstaaten stellen sicher, dass die Absätze 1 bis 5 des vorliegenden Artikels nicht gelten für

a) Zahlungsdienstleister im Sinne des Artikels 1 Absatz 1 Buchstaben a, b und d,

b) Kontoinformationsdienstleister im Sinne des Artikels 33 Absatz 1,

c) Zahlungsinstitute, die gemäß Artikel 32 Absatz 1 ausgenommen sind, und

d) E-Geld-Institute, für die eine Ausnahme gemäß Artikel 9 Absatz 1 der Richtlinie 2009/110/EG gilt."

6. Artikel 98 Absatz 5 erhält folgende Fassung:

„(5) Gemäß Artikel 10 der Verordnung (EU) Nr. 1093/2010 überprüft und aktualisiert die EBA — soweit erforderlich — die technischen Regulierungsstandards regelmäßig, um unter anderem der Innovation und den technologischen Entwicklungen sowie den Bestimmungen des Kapitels II der Verordnung (EU) 2022/2554 Rechnung zu tragen."

*Artikel 8*

**Änderung der Richtlinie (EU) 2016/2341**

Artikel 21 Absatz 5 der Richtlinie (EU) 2016/2341 erhält folgende Fassung:

„(5) Die Mitgliedstaaten stellen sicher, dass die EbAV angemessene Vorkehrungen treffen, einschließlich der Entwicklung von Notfallplänen, um die Kontinuität und Ordnungsmäßigkeit ihrer Tätigkeiten zu gewährleisten.

Gegebenenfalls greifen die EbAV zu diesem Zweck auf geeignete und verhältnismäßige Systeme, Ressourcen und Verfahren zurück, richten insbesondere Netzwerk- und Informationssysteme ein und verwalten diese gemäß der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates (*).

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

*Artikel 9*

**Umsetzung**

(1) Spätestens am 17. Januar 2025 erlassen und veröffentlichen die Mitgliedstaaten die Maßnahmen, die erforderlich sind, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Maßnahmen ab dem 17. Januar 2025 an.

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

(2) Die Mitgliedstaaten teilen der Kommission den Wortlaut der wichtigsten nationalen Maßnahmen mit, die sie auf dem unter diese Richtlinie fallenden Gebiet erlassen.

*Artikel 10*

**Inkrafttreten**

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

*Artikel 11*

**Adressaten**

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 14. Dezember 2022.

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

# RICHTLINIE (EU) 2022/2557 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

## vom 14. Dezember 2022

## über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates

**(Text von Bedeutung für den EWR)**

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

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

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

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

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

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) In einer zunehmend verflochtenen Unionswirtschaft kommt kritischen Einrichtungen als Anbietern wesentlicher Dienste eine unverzichtbare Rolle bei der Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten im Binnenmarkt zu. Daher ist es von wesentlicher Bedeutung, einen Unionsrahmen zu schaffen, der sowohl darauf abzielt, die Resilienz kritischer Einrichtungen im Binnenmarkt durch die Festlegung harmonisierter Mindestverpflichtungen zu verbessern, als auch darauf, diesen Einrichtungen durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu helfen.

(2) In der Richtlinie 2008/114/EG des Rates ([4]) ist ein Verfahren für die Ausweisung europäischer kritischer Infrastrukturen im Energiesektor und im Verkehrssektor vorgesehen, deren Störung oder Zerstörung erhebliche grenzüberschreitende Auswirkungen in mindestens zwei Mitgliedstaaten hätte. Den Schwerpunkt jener Richtlinie bildet ausschließlich der Schutz solcher Infrastrukturen. Bei der im Jahr 2019 durchgeführten Evaluierung der Richtlinie 2008/114/EG wurde jedoch festgestellt, dass aufgrund des zunehmend vernetzten und grenzüberschreitenden Charakters von Tätigkeiten, bei denen kritische Infrastrukturen genutzt werden, Schutzmaßnahmen für einzelne Objekte allein nicht ausreichen, um alle Störungen zu verhindern. Deshalb muss der Ansatz geändert und mit ihm sichergestellt werden, dass Risiken besser berücksichtigt werden, dass die Aufgaben und die Pflichten der kritischen Einrichtungen als Anbieter von Diensten, die für das Funktionieren des Binnenmarkts wesentlich

([1]) ABl. C 286 vom 16.7.2021, S. 170.
([2]) ABl. C 440 vom 29.10.2021, S. 99.
([3]) Standpunkt des Europäischen Parlaments vom 22. November 2022 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 8. Dezember 2022.
([4]) Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern (ABl. L 345 vom 23.12.2008, S. 75).

sind, genauer festgelegt werden und kohärent sind und dass Unionsvorschriften angenommen werden, um die Resilienz kritischer Einrichtungen zu verbessern. So sollten kritische Einrichtungen in der Lage sein, ihre Fähigkeit zu stärken, Sicherheitsvorfälle, die die Erbringung wesentlicher Dienste stören könnten, zu verhindern, sich davor zu schützen, darauf zu reagieren, sie abzuwehren, zu begrenzen, aufzufangen, zu bewältigen und sich von solchen Vorfällen zu erholen.

(3) Zwar wird mit einer Reihe von Maßnahmen sowohl auf Unionsebene, wie das Europäische Programm für den Schutz kritischer Infrastrukturen, als auch auf nationaler Ebene die Unterstützung des Schutzes kritischer Infrastrukturen in der Union angestrebt, jedoch sollte noch mehr unternommen werden, um die Einrichtungen, die solche Infrastrukturen betreiben, besser auszustatten, um auf Risiken für ihren Betrieb reagieren zu können, die zur Störung der Erbringung von wesentlichen Diensten führen könnten. Es sollte auch mehr unternommen werden, damit diese Einrichtungen besser ausgestattet sind, da eine dynamische Bedrohungslage besteht, die sich wandelnde hybride und terroristische Bedrohungen sowie wachsende gegenseitige Abhängigkeiten zwischen Infrastrukturen und Sektoren einschließt. Ferner besteht ein erhöhtes physisches Risiko im Zusammenhang mit Naturkatastrophen und dem Klimawandel, der die Häufigkeit und das Ausmaß von Wetterextremen erhöht und zu langfristigen Veränderungen der durchschnittlichen Klimaverhältnisse führt, die die Kapazität, Effizienz und Lebensdauer bestimmter Infrastrukturarten verringern können, wenn keine Maßnahmen zur Anpassung an den Klimawandel getroffen werden. Darüber hinaus erfolgt die Ermittlung kritischer Einrichtungen im Binnenmarkt uneinheitlich, denn die entsprechenden Sektoren und Kategorien von Einrichtungen werden nicht in allen Mitgliedstaaten kohärent als kritisch eingestuft. Mit dieser Richtlinie sollte daher ein solides Maß an Harmonisierung in Bezug auf die in ihren Anwendungsbereich fallenden Sektoren und Kategorien von Einrichtungen erreicht werden.

(4) Während bestimmte Wirtschaftssektoren wie der Energiesektor und der Verkehrssektor bereits durch sektorspezifische Rechtsakte der Union reguliert sind, enthalten diese Rechtsakte Bestimmungen, die nur bestimmte Aspekte der Resilienz der in diesen Sektoren tätigen Einrichtungen betreffen. Um die Resilienz der Einrichtungen, die für das reibungslose Funktionieren des Binnenmarkts von entscheidender Bedeutung sind, umfassend anzugehen, schafft diese Richtlinie einen übergreifenden Rahmen, der die Resilienz kritischer Einrichtungen gegenüber allen — durch Naturkatastrophen oder vom Menschen verursachten, unbeabsichtigten oder vorsätzlichen — Gefahren berücksichtigt.

(5) Die wachsenden gegenseitigen Abhängigkeiten zwischen Infrastrukturen und Sektoren sind das Ergebnis eines sich über immer mehr Grenzen hinweg erstreckenden und zunehmend verflochtenen Dienstleistungsnetzes, das wichtige Infrastrukturen in der gesamten Union nutzt, und zwar in den Sektoren Energie, Verkehr, Banken, Trinkwasser, Abwasser, Produktion, Verarbeitung und Vertrieb von Lebensmitteln, Gesundheit, Weltraum, Finanzmarktinfrastruktur sowie digitale Infrastruktur als auch in bestimmten Bereichen der öffentlichen Verwaltung. Der Weltraumsektor fällt in den Anwendungsbereich dieser Richtlinie in Bezug auf die Erbringung bestimmter Dienste, die von Bodeninfrastrukturen abhängig sind, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden; folglich fallen Infrastrukturen, die sich im Eigentum der Union befinden oder von der Union oder in ihrem Namen im Rahmen ihres Weltraumprogramms verwaltet oder betrieben werden, nicht in den Anwendungsbereich dieser Richtlinie.

Für den Energiesektor und insbesondere die Methoden der Elektrizitätserzeugung und -übertragung (in Bezug auf die Stromversorgung) gilt, dass — sofern dies als zweckmäßig erachtet wird — der Begriff Elektrizitätserzeugung auch die zur Übertragung von Elektrizität verwendeten Komponenten von Kernkraftwerken abdecken kann, nicht jedoch die spezifisch kerntechnischen Komponenten, die durch Verträge und das Unionsrecht, einschließlich der entsprechenden Rechtsvorschriften der Union im Nuklearbereich, erfasst werden. Der Prozess zur Ermittlung kritischer Einrichtungen im Lebensmittelsektor sollte der Art des Binnenmarktes in diesem Sektor und den umfassenden Unionsvorschriften in Bezug auf die allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts und der Lebensmittelsicherheit angemessen Rechnung tragen. Um daher einen verhältnismäßigen Ansatz sicherzustellen und die Rolle und Bedeutung jener Einrichtungen auf nationaler Ebene angemessen widerzuspiegeln, sollten kritische Einrichtungen daher nur unter Lebensmittelunternehmen ermittelt werden — unabhängig davon, ob sie gewinnorientiert sind oder nicht und ob es sich um öffentliche oder private Unternehmen handelt —, die ausschließlich in den Bereichen Logistik und Großhandel sowie industrielle Großproduktion und -verarbeitung mit einem auf nationaler Ebene beobachteten erheblichen Marktanteil tätig sind. Wegen dieser gegenseitigen Abhängigkeiten kann jede Störung wesentlicher Dienste, auch wenn sie anfänglich auf eine Einrichtung oder einen Sektor beschränkt ist, zu breiteren Kaskadeneffekten führen, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können. Größere Krisen wie die COVID-19-Pandemie haben gezeigt, wie anfällig unsere zunehmend verflochtenen Gesellschaften für Risiken mit erheblichen Auswirkungen und geringer Eintrittswahrscheinlichkeit sind.

(6) Die an der Erbringung wesentlicher Dienste beteiligten Einrichtungen unterliegen zunehmend unterschiedlichen Anforderungen, die sich aus nationalem Recht ergeben. Der Umstand, dass in einigen Mitgliedstaaten weniger strenge Sicherheitsanforderungen für diese Einrichtungen gelten, führt nicht nur zu unterschiedlichen Resilienzniveaus, sondern bringt auch das Risiko negativer Auswirkungen auf die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten in der gesamten Union mit sich und führt ferner auch zu Hindernissen für das reibungslose Funktionieren des Binnenmarkts. Investoren und Unternehmen können sich auf resiliente kritische Einrichtungen verlassen und ihnen vertrauen, und Zuverlässigkeit und Vertrauen sind die Eckpfeiler eines gut funktionierenden Binnenmarkts. Ähnliche Arten von Einrichtungen gelten in einigen Mitgliedstaaten als kritisch, in anderen jedoch nicht, und selbst die als kritisch eingestuften Einrichtungen unterliegen in verschiedenen Mitgliedstaaten unterschiedlichen Anforderungen. Dies führt zu zusätzlichem und unnötigem Verwaltungsaufwand für grenzüberschreitend tätige Unternehmen, insbesondere für solche, die in Mitgliedstaaten mit strengeren Anforderungen tätig sind. Ein Unionsrahmen würde daher auch dazu führen, dass die Wettbewerbsbedingungen für kritische Einrichtungen in der gesamten Union angeglichen werden.

(7) Um die Erbringung wesentlicher Dienste im Binnenmarkt sicherzustellen, die Resilienz kritischer Einrichtungen zu erhöhen und die grenzüberschreitende Zusammenarbeit zwischen den zuständigen Behörden zu verbessern, müssen harmonisierte Mindestvorschriften festgelegt werden. Es ist wichtig, dass diese Vorschriften in Bezug auf ihre Gestaltung und Umsetzung zukunftstauglich sind und gleichzeitig die notwendige Flexibilität bieten. Es ist auch von erheblicher Bedeutung, die Kapazitäten kritischer Einrichtungen für die Erbringung wesentlicher Dienste angesichts vielfältiger Risiken zu verbessern.

(8) Um ein hohes Resilienzniveau zu erreichen, sollten die Mitgliedstaaten kritische Einrichtungen ermitteln, die einerseits besonderen Anforderungen und einer spezifischen Aufsicht unterliegen werden, und die andererseits gegenüber allen entsprechenden Risiken in besonderem Maße unterstützt und mit Leitfäden ausgestattet werden sollen.

(9) Angesichts der Bedeutung der Cybersicherheit für die Resilienz kritischer Einrichtungen und im Sinne der Einheitlichkeit sollte möglichst dafür gesorgt werden, dass der Ansatz dieser Richtlinie und der Ansatz der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([5]) kohärent sind. Im Hinblick auf die häufiger auftretenden Cyberrisiken und ihre besonderen Merkmale sieht die Richtlinie (EU) 2022/2555 für eine Vielzahl von Einrichtungen umfassende Anforderungen vor, die ihre Cybersicherheit gewährleisten sollen. Da die Richtlinie (EU) 2022/2555 das Thema Cybersicherheit ausreichend abdeckt, sollte der Inhalt jener Richtlinie unbeschadet der besonderen Regelungen für Einrichtungen, die im Bereich der digitalen Infrastruktur tätig sind, vom Anwendungsbereich der vorliegenden Richtlinie ausgenommen werden.

(10) Wenn kritische Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union Maßnahmen zur Verbesserung ihrer Resilienz ergreifen müssen und diese Anforderungen den entsprechenden Verpflichtungen aus dieser Richtlinie von den Mitgliedstaaten als zumindest gleichwertig anerkannt sind, sollten die entsprechenden Bestimmungen dieser Richtlinie keine Anwendung finden, damit Doppelarbeit und unnötiger Aufwand vermieden werden. In diesem Fall sollten die in diesen Rechtsakten der Union festgelegten entsprechenden Bestimmungen Anwendung finden. Wenn die entsprechenden Bestimmungen dieser Richtlinie nicht anwendbar sind, sollten auch die in dieser Richtlinie festgelegten Aufsichts- und Durchsetzungsbestimmungen nicht anwendbar sein.

(11) Diese Richtlinie berührt nicht die Zuständigkeit der Mitgliedstaaten und ihrer Behörden hinsichtlich der Verwaltungsautonomie oder ihre Verantwortung für den Schutz der nationalen Sicherheit und Verteidigung oder ihre Befugnis zum Schutz anderer wesentlicher staatlicher Funktionen, insbesondere in Bezug auf die öffentliche Sicherheit, die territoriale Unversehrtheit und die Aufrechterhaltung der öffentlichen Ordnung. Der Ausschluss von Einrichtungen der öffentlichen Verwaltung vom Anwendungsbereich dieser Richtlinie sollte für Einrichtungen gelten, deren Tätigkeiten überwiegend in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten, ausgeübt werden. Jedoch sollten Einrichtungen der öffentlichen Verwaltung, deren Tätigkeiten nur geringfügig mit diesen Bereichen zusammenhängen, in den Anwendungsbereich dieser Richtlinie fallen. Für die Zwecke dieser Richtlinie gelten Einrichtungen mit Regulierungsbefugnissen nicht als Einrichtungen, die Tätigkeiten im Bereich der Strafverfolgung ausüben, und sind demnach nicht vom Anwendungsbereich dieser Richtlinie ausgenommen. Einrichtungen der öffentlichen Verwaltung, die im Einklang mit einer internationalen Übereinkunft gemeinsam mit einem Drittland errichtet wurden, fallen nicht in den Anwendungsbereich dieser Richtlinie. Diese Richtlinie gilt nicht für die diplomatischen und die konsularischen Vertretungen der Mitgliedstaaten in Drittländern.

([5]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (siehe Seite 80 dieses Amtsblatts).

Bestimmte kritische Einrichtungen üben Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten, aus oder erbringen ausschließlich Dienste für Einrichtungen der öffentlichen Verwaltung, die hauptsächlich in diesen Bereichen tätig sind. Im Hinblick auf die Verantwortung der Mitgliedstaaten für den Schutz der nationalen Sicherheit und Verteidigung sollten die Mitgliedstaaten beschließen können, dass die in dieser Richtlinie festgelegten Verpflichtungen für kritische Einrichtungen weder ganz noch teilweise für jene kritischen Einrichtungen gelten sollten, wenn die von ihnen erbrachten Dienste oder ausgeübten Tätigkeiten überwiegend mit den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten, zusammenhängen. Kritische Einrichtungen, deren Dienste oder Tätigkeiten nur geringfügig mit diesen Bereichen in Zusammenhang stehen, sollten in den Anwendungsbereich dieser Richtlinie fallen. Kein Mitgliedstaat sollte verpflichtet sein, Informationen bereitzustellen, deren Offenlegung seinen wesentlichen Interessen in Bezug auf seine nationale Sicherheit zuwiderlaufen würde. Unions- oder nationale Vorschriften zum Schutz von Verschlusssachen sowie Geheimhaltungsvereinbarungen sind von Belang.

(12) Um die nationale Sicherheit bzw. die Sicherheit und die geschäftlichen Interessen kritischer Einrichtungen nicht zu gefährden, sollte der Zugang zu sensiblen Informationen, ihr Austausch und der Umgang mit ihnen umsichtig und mit besonderem Augenmerk auf die verwendeten Übertragungskanäle und Speicherkapazitäten erfolgen.

(13) Im Hinblick auf die Gewährleistung eines umfassenden Ansatzes in Bezug auf die Resilienz kritischer Einrichtungen sollte jeder Mitgliedstaat über eine Strategie zur Verbesserung der Resilienz kritischer Einrichtungen (im Folgenden „Strategie“) verfügen. Die Strategien sollten die umzusetzenden strategischen Ziele und politischen Maßnahmen festlegen. Im Interesse von Kohärenz und Effizienz sollte die Strategie so konzipiert sein, dass bestehende politische Strategien nahtlos einbezogen werden, wobei nach Möglichkeit auf entsprechenden bestehenden nationalen und sektorbezogenen Strategien, Plänen oder ähnlichen Dokumenten aufgebaut werden sollte. Zur Verwirklichung eines umfassenden Ansatzes sollten die Mitgliedstaaten sicherstellen, dass ihre Strategien in Bezug auf den Informationsaustausch über Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle und über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle sowie im Zusammenhang mit der Wahrnehmung von Aufsichtsaufgaben einen Rahmen für eine verstärkte Koordinierung zwischen der gemäß der vorliegenden Richtlinie zuständigen Behörde und der gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörde vorsehen. Bei der Einführung ihrer Strategien sollten die Mitgliedstaaten dem hybriden Charakter von Bedrohungen für kritische Einrichtungen gebührend Rechnung tragen.

(14) Die Mitgliedstaaten sollten der Kommission ihre Strategien und deren wesentliche Aktualisierungen mitteilen, um insbesondere die Kommission in die Lage zu versetzen, die ordnungsgemäße Anwendung dieser Richtlinie in Bezug auf politische Ansätze für die Resilienz kritischer Einrichtungen auf nationaler Ebene zu bewerten. Die Strategien könnten erforderlichenfalls als Verschlusssache übermittelt werden. Die Kommission sollte einen zusammenfassenden Bericht über die von den Mitgliedstaaten übermittelten Strategien erstellen, der als Grundlage für den Austausch dienen soll, um bewährte Verfahren und Fragen von gemeinsamem Interesse im Rahmen einer Gruppe für die Resilienz kritischer Einrichtungen zu ermitteln. In Anbetracht der Sensibilität der im zusammenfassenden Bericht enthaltenen aggregierten Informationen — unabhängig davon, ob sie als Verschlusssache eingestuft sind oder nicht —, sollte die Kommission den zusammenfassenden Bericht mit dem angemessenen Maß an Bewusstsein für die Sicherheit der kritischen Einrichtungen, der Mitgliedstaaten und der Union verwalten. Damit die Ziele dieser Richtlinie erreicht werden, sollten der zusammenfassende Bericht und die Strategien vor rechtswidrigen oder böswilligen Handlungen geschützt werden und nur befugten Personen zugänglich sein. Die Übermittlung der Strategien und ihrer wesentlichen Aktualisierungen sollte auch dazu beitragen, dass die Kommission, die Entwicklungen bei den Ansätzen für die Resilienz kritischer Einrichtungen versteht, und in die Überwachung der Auswirkungen und des Mehrwerts dieser Richtlinie einfließen, die die Kommission regelmäßig zu überprüfen hat.

(15) Die Maßnahmen der Mitgliedstaaten zur Ermittlung der kritischen Einrichtungen und zur Gewährleistung ihrer Resilienz sollten einem risikobasierten Ansatz folgen, bei dem diejenigen Einrichtungen im Fokus stehen, die für die Erfüllung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten am bedeutendsten sind. Um einen solchen gezielten Ansatz zu ermöglichen, sollte jeder Mitgliedstaat innerhalb eines harmonisierten Rahmens eine Bewertung der entsprechenden natürlichen und vom Menschen verursachten Risiken — einschließlich Risiken grenzüberschreitender oder sektorübergreifender Art — vornehmen, die sich auf die Erbringung wesentlicher Dienste auswirken könnten, wie Unfälle, Naturkatastrophen, gesundheitliche Notlagen wie etwa Pandemien und hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, krimineller Unterwanderung und Sabotage (im Folgenden „Risikobewertung durch Mitgliedstaaten“). Bei der Durchführung von Risikobewertungen durch Mitgliedstaaten sollten die Mitgliedstaaten andere allgemeine oder sektorspezifische Risikobewertungen berücksichtigen, die gemäß anderen Unionsrechtsakten durchgeführt werden, und das Ausmaß der Abhängigkeit zwischen Sektoren, auch in Bezug auf Sektoren in anderen Mitgliedstaaten und Drittländern, Rechnung tragen. Die Ergebnisse der Risikobewertungen durch Mitgliedstaaten sollten bei der Ermittlung kritischer

Einrichtungen verwendet werden sowie dazu, diese bei der Erfüllung ihrer Resilienzanforderungen zu unterstützen. Diese Richtlinie gilt nur für die Mitgliedstaaten und für die kritischen Einrichtungen, die in der Union tätig sind. Dennoch könnten die Fachkenntnisse und das Wissen, die von den zuständigen Behörden, insbesondere durch Risikobewertungen, sowie von der Kommission, insbesondere durch verschiedene Formen der Unterstützung und Zusammenarbeit, gewonnen werden, gegebenenfalls und im Einklang mit den geltenden Rechtsinstrumenten zugunsten von Drittländern — insbesondere derjenigen in der unmittelbaren Nachbarschaft der Union — genutzt werden, indem sie in die bestehende Zusammenarbeit im Bereich der Resilienz einfließen.

(16) Um sicherzustellen, dass alle entsprechenden Einrichtungen den Resilienzanforderungen dieser Richtlinie unterliegen, und um diesbezügliche Unterschiede zu verringern, ist es wichtig, harmonisierte Vorschriften festzulegen, die eine einheitliche Ermittlung kritischer Einrichtungen in der gesamten Union ermöglichen und die es den Mitgliedstaaten dennoch auch erlauben, den Aufgaben und der Bedeutung dieser Einrichtungen auf nationaler Ebene angemessen Rechnung zu tragen. Unter Anwendung der in dieser Richtlinie festgelegten Kriterien sollte jeder Mitgliedstaat Einrichtungen ermitteln, die einen oder mehrere wesentliche Dienste erbringen und die in seinem Hoheitsgebiet tätig sind und ihre kritischen Infrastrukturen befinden sich dort. Es sollte davon ausgegangen werden, dass eine Einrichtung im Hoheitsgebiet des Mitgliedstaats tätig ist, in dem sie Tätigkeiten ausübt, die für den betreffenden wesentlichen Dienst bzw. für die betreffenden wesentlichen Dienste erforderlich sind, und in dem sich die kritische Infrastruktur dieser Einrichtung, die zur Erbringung dieses Dienstes bzw. dieser Dienste genutzt wird, befindet. Wenn es in einem Mitgliedstaat keine Einrichtung gibt, die diese Kriterien erfüllt, sollte dieser Mitgliedstaat nicht verpflichtet sein, eine kritische Einrichtung in dem entsprechenden Sektor oder Teilsektor zu ermitteln. Im Interesse der Wirksamkeit, Effizienz, Kohärenz und Rechtssicherheit sollten geeignete Vorschriften festgelegt werden, um Einrichtungen mitzuteilen, dass sie als kritische Einrichtungen eingestuft wurden.

(17) Die Mitgliedstaaten sollten der Kommission in einer Form, die die Ziele dieser Richtlinie erfüllt, eine Liste der wesentlichen Dienste, die Anzahl der für jeden der im Anhang genannten Sektoren und Teilsektoren ermittelten kritischen Einrichtungen und für den bzw. die von jeder Einrichtung geleisteten wesentlichen Dienst bzw. Dienste sowie die gegebenenfalls angewandten Schwellenwerte übermitteln. Schwellenwerte sollten als solche oder in aggregierter Form dargestellt werden können, d. h. die Informationen können gemittelt nach geografischem Gebiet, Jahr, Sektor, Teilsektor oder nach anderen Kriterien angegeben werden und Informationen über die Bandbreite der angegebenen Indikatoren enthalten.

(18) Es sollten Kriterien festgelegt werden, um das Ausmaß einer durch einen Sicherheitsvorfall verursachten Störung zu bestimmen. Diese Kriterien sollten sich an den in der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([6]) festgelegten Kriterien orientieren, um die Anstrengungen der Mitgliedstaaten zur Ermittlung der Betreiber wesentlicher Dienste im Sinne jener Richtlinie und die diesbezüglich gewonnenen Erfahrungen zu nutzen. Schwere Krisen wie die COVID-19-Pandemie haben gezeigt, wie wichtig es ist, die Sicherheit der Lieferketten zu gewährleisten, und wie deren Unterbrechung negative wirtschaftliche und gesellschaftliche Auswirkungen in sehr vielen Sektoren und auf grenzüberschreitender Ebene haben kann. Daher sollten die Mitgliedstaaten bei der Bestimmung des Ausmaßes der Abhängigkeit anderer Sektoren und Teilsektoren von wesentlichen Diensten einer kritischen Einrichtung so weit wie möglich auch die Auswirkungen auf die Lieferketten berücksichtigen.

(19) Im Einklang mit geltendem Unionsrecht und nationalem Recht, einschließlich der Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates ([7]), mit der ein Rahmen für die Überprüfung ausländischer Direktinvestitionen in der Union geschaffen wurde, muss die potenzielle Bedrohung durch ausländische Beteiligungen an kritischen Infrastrukturen in der Union anerkannt werden, da Dienste, die Wirtschaft, die Freizügigkeit und die Sicherheit der Unionsbürgerinnen und Unionsbürger vom ordnungsgemäßen Funktionieren der kritischen Infrastrukturen abhängen.

(20) Mit der Richtlinie (EU) 2022/2555 werden Einrichtungen im Bereich digitale Infrastruktur, die für eine Einstufung als kritische Einrichtungen im Sinne dieser Richtlinie in Frage kommen könnten, verpflichtet, geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit von Netz- und Informationssystemen zu beherrschen, und erhebliche Sicherheitsvorfälle und Cyberbedrohungen zu melden. Da Gefahren für die Sicherheit von Netz- und Informationssystemen unterschiedliche Ursachen haben können, wird in der Richtlinie (EU) 2022/2555 ein „gefahrenübergreifender" Ansatz angewandt, der die Resilienz von Netz- und Informationssystemen sowie die physischen Komponenten und das physische Umfeld dieser Systeme umfasst.

([6]) 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).

([7]) Verordnung (EU) 2019/452 des Europäischen Parlaments und des Rates vom 19. März 2019 zur Schaffung eines Rahmens für die Überprüfung ausländischer Direktinvestitionen in der Union (ABl. L 79 I vom 21.3.2019, S. 1).

Da die in der Richtlinie (EU) 2022/2555 diesbezüglich festgelegten Anforderungen den entsprechenden Verpflichtungen aus dieser Richtlinie zumindest gleichwertig sind, sollten die in Artikel 11 und in Kapitel III, IV und VI dieser Richtlinie festgelegten Verpflichtungen für Einrichtungen im Bereich digitale Infrastruktursektor nicht gelten, damit Doppelarbeit und unnötiger Verwaltungsaufwand vermieden werden. Angesichts dessen, dass die von Einrichtungen im Bereich digitale Infrastruktur erbrachten Dienste für kritische Einrichtungen aller anderen Wirtschaftssektoren sehr wichtig sind, sollten die Mitgliedstaaten jedoch auf der Grundlage der in der vorliegenden Richtlinie vorgesehenen Kriterien und Verfahren auch Einrichtungen im Bereich digitale Infrastruktur als kritische Einrichtungen ermitteln. Folglich sollten die Strategien, die Risikobewertungen durch Mitgliedstaaten und die Unterstützungsmaßnahmen gemäß Kapitel II dieser Richtlinie Anwendung finden. Die Mitgliedstaaten sollten in der Lage sein, nationale Vorschriften zu erlassen oder beizubehalten, um ein höheres Maß an Resilienz für diese kritischen Einrichtungen zu erreichen, sofern diese Vorschriften mit dem geltenden Unionsrecht vereinbar sind.

(21) Die Rechtsvorschriften der Union für Finanzdienstleistungen enthalten umfassende Anforderungen für Finanzunternehmen in Bezug auf die Steuerung aller ihrer Risiken, einschließlich der operationellen Risiken, und die Aufrechterhaltung des Betriebs. Diese Rechtsvorschriften umfassen die Verordnungen (EU) Nr. 648/2012 ([8]) (EU) Nr. 575/2013 ([9]) und (EU) Nr. 600/2014 ([10]) des Europäischen Parlaments und des Rates und die Richtlinien 2013/36/EU ([11]) und 2014/65/EU ([12]) des Europäischen Parlaments und des Rates. Dieser Rechtsrahmen wird durch die Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates ([13]) ergänzt, in der Anforderungen an Finanzunternehmen in Bezug auf den Umgang mit Risiken der Informations- und Kommunikationstechnologie (IKT) und einschließlich hinsichtlich des Schutzes physischer IKT-Infrastrukturen festgelegt sind. Da die Resilienz dieser Einrichtungen daher umfassend abgedeckt wird, sollten Artikel 11 und die Kapitel III, IV und VI dieser Richtlinie nicht für diese Einrichtungen gelten, damit Doppelarbeit und unnötiger Verwaltungsaufwand vermieden werden.

In Anbetracht dessen, dass die von Einrichtungen im Finanzsektor erbrachten Dienste für kritische Einrichtungen aller anderen Wirtschaftssektoren sehr wichtig sind, sollten die Mitgliedstaaten jedoch auf der Grundlage der in der vorliegenden Richtlinie vorgesehenen Kriterien und Verfahren auch im Finanzsektor tätige Einrichtungen als kritische Einrichtungen ermitteln. Folglich sollten die Strategien, die Risikobewertungen durch Mitgliedstaaten und die Unterstützungsmaßnahmen gemäß Kapitel II dieser Richtlinie Anwendung finden. Die Mitgliedstaaten sollten in der Lage sein, nationale Rechtsvorschriften zu erlassen oder beizubehalten, um ein höheres Maß an Resilienz für diese kritischen Einrichtungen zu erreichen, sofern diese Vorschriften mit dem geltenden Unionsrecht vereinbar sind.

(22) Die Mitgliedstaaten sollten Behörden benennen oder einrichten, die für die Überwachung der Anwendung dieser Richtlinie und erforderlichenfalls für die Durchsetzung ihrer Vorschriften zuständig sind, und dafür sorgen, dass diese Behörden über angemessene Befugnisse und Ressourcen verfügen. Angesichts der unterschiedlichen nationalen Verwaltungsstrukturen, um bestehende sektorbezogene Vereinbarungen oder Aufsichts- und Regulierungsstellen der Union beizubehalten und um Doppelarbeit zu vermeiden, sollten die Mitgliedstaaten befugt sein, mehr als eine zuständige Behörde zu benennen oder einzurichten. Wenn die Mitgliedstaaten mehr als eine zuständige Behörde benennen oder einrichten, sollten sie die jeweiligen Aufgaben der betreffenden Behörden klar abgrenzen und sicherstellen, dass sie reibungslos und wirksam zusammenarbeiten. Alle zuständigen Behörden sollten auch generell sowohl auf Unionsebene als auch auf nationaler Ebene mit anderen entsprechenden Behörden zusammenarbeiten.

([8]) 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).

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

([10]) Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 173 vom 12.6.2014, S. 84).

([11]) Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG (ABl. L 176 vom 27.6.2013, S. 338).

([12]) 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).

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

(23) Zur Erleichterung der grenzüberschreitenden Zusammenarbeit und Kommunikation, und um die effektive Umsetzung dieser Richtlinie zu ermöglichen, sollte jeder Mitgliedstaat unbeschadet der Anforderungen der sektorbezogenen Rechtsakte der Union eine — gegebenenfalls innerhalb einer zuständigen Behörde angesiedelte — zentrale Anlaufstelle benennen, die für die Koordinierung von Fragen im Zusammenhang mit der Resilienz kritischer Einrichtungen und für die grenzüberschreitende Zusammenarbeit auf Unionsebene zuständig ist (im Folgenden „zentrale Anlaufstelle"). Jede zentrale Anlaufstelle sollte mit den zuständigen Behörden ihres Mitgliedstaats, mit den zentralen Anlaufstellen anderer Mitgliedstaaten und mit der Gruppe für die Resilienz kritischer Einrichtungen in Kontakt stehen und gegebenenfalls die Kommunikation mit ihnen abstimmen.

(24) Die gemäß der vorliegenden Richtlinie und gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden sollten in Bezug auf Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle sowie nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle, die kritische Einrichtungen betreffen, und in Bezug auf entsprechende Maßnahmen, die von gemäß der vorliegenden Richtlinie und der Richtlinie 2022/2555 zuständigen Behörden ergriffen werden, zusammenarbeiten und Informationen austauschen. Es ist wichtig, dass die Mitgliedstaaten sicherstellen, dass die Anforderungen nach der vorliegenden Richtlinie und der Richtlinie (EU) 2022/2555 komplementär umgesetzt werden und dass kritische Einrichtungen keinem Verwaltungsaufwand ausgesetzt sind, der über das zur Erreichung der Ziele dieser und jener Richtlinie erforderliche Maß hinausgeht.

(25) Unbeschadet der eigenen rechtlichen Verantwortung der kritischen Einrichtungen, die in der vorliegenden Richtlinie enthaltenen Verpflichtungen einzuhalten, sollten die Mitgliedstaaten die kritischen Einrichtungen, insbesondere jene, die als kleine oder mittlere Unternehmen einzustufen sind, im Einklang mit den Verpflichtungen von Mitgliedstaaten aus der vorliegenden Richtlinie beim Ausbau ihrer Resilienz unterstützen und dabei übermäßigem Verwaltungsaufwand vorbeugen. Die Mitgliedstaaten könnten insbesondere Leitfäden und Methoden für ihre kritischen Einrichtungen entwickeln, sie bei der Organisation von Übungen zur Überprüfung der Resilienz kritischer Einrichtungen unterstützen sowie Beratung und Schulungen für das Personal kritischer Einrichtungen bereitstellen. Sofern dies erforderlich und durch Ziele des Allgemeininteresses gerechtfertigt ist, könnten die Mitgliedstaaten Finanzmittel bereitstellen und sollten unbeschadet der Anwendung der im Vertrag über die Arbeitsweise der Europäischen Union (AEUV) festgelegten Wettbewerbsregeln den freiwilligen Informationsaustausch und den Austausch bewährter Verfahren zwischen kritischen Einrichtungen erleichtern.

(26) Um die Resilienz der von den Mitgliedstaaten ermittelten kritischen Einrichtungen zu verbessern und den Verwaltungsaufwand für diese kritischen Einrichtungen zu verringern, sollten die zuständigen Behörden einander gegebenenfalls zur Sicherstellung einer einheitlichen Anwendung dieser Richtlinie konsultieren. Diese Konsultationen sollten auf Antrag jeder interessierten zuständigen Behörde aufgenommen werden, und sie sollten darauf ausgerichtet sein, einen konvergenten Ansatz bezüglich miteinander verknüpfter kritischer Einrichtungen sicherzustellen, die kritische Infrastrukturen mit physischen Verbindungen zwischen zwei oder mehr Mitgliedstaaten nutzen, die derselben Gruppe oder Unternehmensstruktur angehören oder die in einem Mitgliedstaat ermittelt wurden und die wesentliche Dienste für andere oder in anderen Mitgliedstaaten erbringen.

(27) Sind kritische Einrichtungen aufgrund von Bestimmungen des Unionsrechts oder des nationalen Rechts verpflichtet, für die Zwecke dieser Richtlinie relevante Risiken zu bewerten und Maßnahmen zur Gewährleistung ihrer eigenen Resilienz zu ergreifen, so sollten diese Anforderungen angemessen berücksichtigt werden, wenn es darum geht zu überwachen, ob kritische Einrichtungen diese Richtlinie einhalten.

(28) Den kritischen Einrichtungen sollten die entsprechenden Risiken, denen sie ausgesetzt sind, in ihrer Gesamtheit bekannt sein, und sie sollten verpflichtet sein, diese Risiken zu analysieren. Zu diesem Zweck sollten sie immer, wenn ihre besondere Situation oder die Entwicklung der Risiken dies erfordern, und in jedem Fall alle vier Jahre Risikobewertungen durchführen, um alle entsprechenden Risiken zu bewerten, die die Erbringung ihrer wesentlichen Dienste stören könnten (im Folgenden „Risikobewertung durch kritische Einrichtungen"). Haben kritische Einrichtungen aufgrund von Verpflichtungen aus anderen Rechtsakten andere Risikobewertungen vorgenommen oder Dokumente erstellt, die für die Risikobewertung durch kritische Einrichtungen nach der vorliegenden Richtlinie relevant sind, so sollten sie diese Bewertungen und Dokumente verwenden können, um die in der vorliegenden Richtlinie hinsichtlich der Risikobewertungen durch kritische Einrichtungen festgelegten Anforderungen zu erfüllen. Eine zuständige Behörde sollte in der Lage sein zu erklären, dass eine, durch eine kritische Einrichtung durchgeführte, bestehende Risikobewertung, die sich mit den entsprechenden Risiken und dem entsprechenden Ausmaß der Abhängigkeiten befasst, ganz oder teilweise den in dieser Richtlinie festgelegten Verpflichtungen entspricht.

(29) Die kritischen Einrichtungen sollten technische, sicherheitsbezogene und organisatorische Maßnahmen ergreifen, die angemessen und geeignet sind für die Risiken, denen sie ausgesetzt sind, und um einen Sicherheitsvorfall zu verhindern, davor zu schützen, darauf zu reagieren, ihn abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, ihn aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen. Während die kritischen Einrichtungen diese Maßnahmen im Einklang mit der vorliegenden Richtlinie ergreifen sollten, sollten die Einzelheiten und der Umfang solcher Maßnahmen die einzelnen Risiken, die jede kritische Einrichtung im Rahmen ihrer Risikobewertung durch kritische Einrichtungen ermittelt hat, und die besondere Situation der betreffenden Einrichtung auf angemessene und verhältnismäßige Weise widerspiegeln. Damit ein einheitlicher Ansatz der Union gefördert wird, sollte die Kommission nach Konsultation der Gruppe für die Resilienz kritischer Einrichtungen nicht verbindliche Leitlinien erlassen, in denen diese technischen, sicherheitsbezogenen und organisatorischen Maßnahmen näher ausgeführt werden. Die Mitgliedstaaten sollten sicherstellen, dass jede kritische Einrichtung einen Verbindungsbeauftragten oder eine Person mit vergleichbarer Aufgabenstellung als Ansprechpartner für die zuständigen Behörden benennt.

(30) Um diese Ziele in Bezug auf die ermittelten Risiken zu erreichen, sollten kritische Einrichtungen die von ihnen ergriffenen Maßnahmen — auch im Interesse der Rechenschaftspflicht und der Wirksamkeit der Maßnahmen — in einem Resilienzplan oder in einem oder mehreren Dokumenten, die einem Resilienzplan gleichwertig sind, hinreichend detailliert beschreiben und diesen Plan in der Praxis anwenden. Hat eine kritische Einrichtung bereits technische, sicherheitsbezogene und organisatorische Maßnahmen ergriffen und Dokumente gemäß anderen Rechtsakten erstellt, die für Maßnahmen zur Verbesserung der Resilienz nach dieser Richtlinie relevant sind, so sollte sie, um Doppelarbeit zu vermeiden, in der Lage sein, diese Maßnahmen und Dokumente zu nutzen, um den Verpflichtungen in Bezug auf die Resilienzmaßnahmen gemäß der vorliegenden Richtlinie nachzukommen. Um Doppelarbeit zu vermeiden, sollte eine zuständige Behörde in der Lage sein, zu erklären, dass bestehende Resilienzmaßnahmen, die von einer kritischen Einrichtung ergriffen wurden, mit denen ihre Verpflichtung, technische, sicherheitsbezogene und organisatorische Maßnahmen gemäß der vorliegenden Richtlinie zu ergreifen, angegangen wird, ganz oder teilweise den Anforderungen dieser Richtlinie entsprechen.

(31) Die Verordnungen (EG) Nr. 725/2004 ([14]) und (EG) Nr. 300/2008 ([15]) des Europäischen Parlaments und des Rates sowie die Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates ([16]) enthalten Verpflichtungen für im Luft- und Seeverkehr tätige Einrichtungen, die darauf abstellen, Sicherheitsvorfälle, die auf rechtswidrige Handlungen zurückzuführen sind, zu verhindern und abzuwehren und die Folgen solcher Vorfälle zu begrenzen. Zwar sind die in dieser Richtlinie geforderten Maßnahmen breiter gefasst, was die zu behandelnden Risiken und die Art der zu ergreifenden Maßnahmen angeht, doch sollten die kritischen Einrichtungen in den betreffenden Sektoren in ihrem Resilienzplan oder gleichwertigen Dokumenten auch auf die gemäß jenen anderen Rechtsakten der Union ergriffenen Maßnahmen eingehen. Kritische Einrichtungen haben auch die Richtlinie 2008/96/EG des Europäischen Parlaments und des Rates ([17]) zu berücksichtigen, mit der eine netzweite Bewertung der Straßen, um die Unfallrisiken abzubilden, sowie eine gezielte Straßensicherheitsüberprüfung eingeführt wird, um auf der Grundlage von Ortsbesichtigungen von bestehenden Straßen oder bestehenden Straßenabschnitten gefährliche Zustände, Mängel und Probleme zu ermitteln, die das Unfall- und Verletzungsrisiko erhöhen. Die Sicherstellung des Schutzes und der Resilienz kritischer Einrichtungen ist für den Eisenbahnsektor von größter Bedeutung, und kritische Einrichtungen werden ermutigt, bei der Umsetzung von Resilienzmaßnahmen nach der vorliegenden Richtlinie auf nicht verbindliche Leitlinien und Dokumente über bewährte Verfahren zu verweisen, die im Rahmen sektorspezifischer Initiativen, wie etwa der durch den Beschluss 2018/C 232/03 der Kommission ([18]) eingerichteten EU-Plattform für die Sicherheit im Schienenpersonenverkehr, ausgearbeitet wurden.

(32) Das Risiko, dass Mitarbeiter kritischer Einrichtungen oder ihre Auftragnehmer beispielsweise ihre Zugangsrechte innerhalb der Organisation der kritischen Einrichtung missbrauchen, um Schaden zu verursachen, gibt zunehmend Anlass zur Sorge. Die Mitgliedstaaten sollten daher die Bedingungen präzisieren, unter denen kritische Einrichtungen in hinreichend begründeten Fällen und unter Berücksichtigung der Risikobewertungen durch Mitgliedstaaten Anträge auf Zuverlässigkeitsüberprüfungen von Personen stellen dürfen, die bestimmten Kategorien ihres Personals angehören. Es sollte sichergestellt werden, dass die entsprechenden Behörden die Anträge innerhalb eines angemessenen Zeitrahmens prüfen und im Einklang mit dem nationalen Recht und den Verfahren sowie mit dem entsprechenden geltenden Unionsrecht, auch hinsichtlich des Schutzes personenbezogener Daten, verarbeiten. Um sich der Identität einer Person zu vergewissern, die einer Zuverlässigkeitsüberprüfung unterzogen wird, ist es angezeigt, dass die Mitgliedstaaten im Einklang mit dem geltenden Recht einen Identitätsnachweis wie einen Reisepass, einen nationalen Personalausweis oder eine digitale Form des Identitätsnachweises verlangen.

---

([14]) 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).

([15]) 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).

([16]) 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).

([17]) Richtlinie 2008/96/EG des Europäischen Parlaments und des Rates vom 19. November 2008 über ein Sicherheitsmanagement für die Straßenverkehrsinfrastruktur (ABl. L 319 vom 29.11.2008, S. 59).

([18]) Beschluss der Kommission vom 29. Juni 2018 zur Einrichtung der EU-Plattform für die Sicherheit im Schienenpersonenverkehr (ABl. C 232 vom 3.7.2018, S. 10).

Solche Zuverlässigkeitsüberprüfungen sollten eine Prüfung des Strafregisters der betreffenden Person einschließen. Mitgliedstaaten sollten das Europäische Strafregisterinformationssystem gemäß den im Rahmenbeschluss 2009/315/JI des Rates ([19]) und — sofern relevant und anwendbar — in der Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates ([20]) festgelegten Verfahren zur Einholung von Informationen aus den Strafregistern von anderen Mitgliedstaaten nutzen. Die Mitgliedstaaten könnten — sofern relevant und anwendbar — auch auf das mit der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates ([21]) eingerichtete Schengener Informationssystem der zweiten Generation (SIS II), auf Erkenntnisse sowie auf sonstige verfügbare objektive Informationen zurückgreifen, die möglicherweise erforderlich sind, um festzustellen, ob die betreffende Person geeignet ist, in der Position zu arbeiten, für die die kritische Einrichtung eine Zuverlässigkeitsüberprüfung beantragt hat.

(33) Es sollte ein Mechanismus für die Meldung bestimmter Sicherheitsvorfälle eingerichtet werden, um es den zuständigen Behörden zu ermöglichen, rasch und angemessen auf Sicherheitsvorfälle zu reagieren und sich einen umfassenden Überblick über die Auswirkungen, die Art, die Ursache und die möglichen Folgen von Sicherheitsvorfällen, die die kritischen Einrichtungen betreffen, zu verschaffen. Kritische Einrichtungen sollten den zuständigen Behörden unverzüglich Sicherheitsvorfälle melden, die die Erbringung wesentlicher Dienste erheblich stören oder erheblich stören könnten. Außer wenn dies in operativer Hinsicht nicht möglich ist, sollten kritische Einrichtungen spätestens 24 Stunden, nachdem sie Kenntnis von einem Sicherheitsvorfall erhalten haben, eine Erstmeldung übermitteln. Die Erstmeldung sollte nur die Informationen enthalten, die unbedingt erforderlich sind, um die zuständige Behörde über den Sicherheitsvorfall zu unterrichten und es der kritischen Einrichtung zu ermöglichen, bei Bedarf Hilfe in Anspruch zu nehmen. In einer solchen Meldung sollte, soweit möglich, die mutmaßliche Ursache des Sicherheitsvorfalls angegeben werden. Die Mitgliedstaaten sollten sicherstellen, dass durch die Pflicht zur Übermittlung dieser Erstmeldung die Ressourcen der kritischen Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, nicht beeinträchtigt werden. Der Erstmeldung sollte gegebenenfalls spätestens einen Monat nach dem Sicherheitsvorfall ein ausführlicher Bericht folgen. Der ausführliche Bericht sollte die ursprüngliche Meldung ergänzen und einen vollständigeren Überblick über den Sicherheitsvorfall bieten.

(34) Die Normung sollte in erster Linie ein marktorientierter Vorgang bleiben. Es gibt jedoch möglicherweise noch immer Situationen, in denen es sich empfiehlt, die Einhaltung bestimmter Normen zu fordern. Die Mitgliedstaaten sollten, wenn dies sinnvoll ist, die Verwendung von europäischen und internationalen Normen und technischen Spezifikationen fördern, die für die Maßnahmen zur Sicherheit und Resilienz kritischer Einrichtungen relevant sind.

(35) Zwar sind kritische Einrichtungen in der Regel als Teil eines immer stärker verflochtenen Dienstleistungs- und Infrastrukturnetzes tätig und erbringen häufig wesentliche Dienste in mehr als einem Mitgliedstaat, doch sind einige dieser kritischen Einrichtungen für die Union und ihren Binnenmarkt von besonderer Bedeutung, da sie wesentliche Dienste für oder in sechs oder mehr Mitgliedstaaten erbringen und daher in den Genuss einer spezifischen Unterstützung auf Unionsebene kommen könnten. Daher sollten für Beratungsmissionen in Bezug auf solche kritischen Einrichtungen, die von besonderer Bedeutung für Europa sind, Vorschriften festgelegt werden. Diese Vorschriften sollten die Aufsichts- und Durchsetzungsvorschriften der vorliegenden Richtlinie unberührt lassen.

(36) Sind zusätzliche Informationen erforderlich, um eine kritische Einrichtung bei der Erfüllung ihrer Verpflichtungen nach dieser Richtlinie beraten zu können oder um zu bewerten, ob eine kritische Einrichtung von besonderer Bedeutung für Europa diese Verpflichtungen erfüllt, so sollte der Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung ermittelt hat, auf ein begründetes Ersuchen der Kommission oder eines oder mehrerer Mitgliedstaaten, für die oder in denen der wesentliche Dienst erbracht wird, der Kommission bestimmte Informationen gemäß der vorliegenden Richtlinie bereitstellen. Die Kommission sollte im Einvernehmen mit dem Mitgliedstaat, der die kritische Einrichtung von besonderer Bedeutung für Europa als eine kritische Einrichtung eingestuft hat, in der Lage sein, eine Beratungsmission zur Bewertung der von dieser Einrichtung ergriffenen Maßnahmen zu organisieren. Um sicherzustellen, dass diese Beratungsmissionen ordnungsgemäß durchgeführt werden, sollten insbesondere in Bezug auf die Organisation und Durchführung von Beratungsmissionen, die zu ergreifenden Folgemaßnahmen und die Verpflichtungen, die sich für die betreffenden

([19]) Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten (ABl. L 93 vom 7.4.2009, S. 23).

([20]) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, sowie zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 135 vom 22.5.2019, S. 1).

([21]) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

kritischen Einrichtungen von besonderer Bedeutung für Europa in diesem Zusammenhang ergeben, ergänzende Vorschriften festgelegt werden. Unbeschadet dessen, dass der Mitgliedstaat, in dem die Beratungsmission durchgeführt wird, sowie die betreffende kritische Einrichtung die in dieser Richtlinie festgelegten Vorschriften einhalten müssen, sollten die Beratungsmissionen den Rechtsvorschriften dieses Mitgliedstaats — beispielsweise über die genauen Bedingungen für den Zugang zu den entsprechenden Räumlichkeiten oder Dokumenten und über Rechtsbehelfe — unterliegen. Das für solche Beratungsmissionen erforderliche spezifische Fachwissen könnte gegebenenfalls über das durch den Beschluss Nr. 1313/2013/EU des Europäischen Parlaments und des Rates ([22]) eingerichtete Zentrum für die Koordination von Notfallmaßnahmen angefordert werden.

(37) Um die Kommission zu unterstützen und die Zusammenarbeit zwischen den Mitgliedstaaten sowie den Austausch von Informationen und bewährten Verfahren zu Fragen im Zusammenhang mit dieser Richtlinie zu erleichtern, sollte eine Gruppe für die Resilienz kritischer Einrichtungen als Expertengruppe der Kommission eingerichtet werden. Die Mitgliedstaaten sollten sich bemühen, eine wirksame und effiziente Zusammenarbeit der benannten Vertreter ihrer zuständigen Behörden in der Gruppe für die Resilienz kritischer Einrichtungen sicherzustellen, indem sie gegebenenfalls Vertreter benennen, die über eine Sicherheitsermächtigung verfügen. Die Gruppe für die Resilienz kritischer Einrichtungen sollte ihre Arbeit so bald wie möglich aufnehmen, damit während der Umsetzungsfrist dieser Richtlinie bereits zusätzliche Mittel für eine angemessene Zusammenarbeit zur Verfügung stehen. Die Gruppe für die Resilienz kritischer Einrichtungen sollte mit anderen entsprechenden sektorspezifischen Expertengruppen interagieren.

(38) Die Gruppe für die Resilienz kritischer Einrichtungen sollte mit der durch die Richtlinie (EU) 2022/2555 eingesetzten Kooperationsgruppe zusammenarbeiten, um einen umfassenden Rahmen für die Cyberresilienz und die nicht cyberbezogene Resilienz kritischer Einrichtungen unterstützen. Die Gruppe für die Resilienz kritischer Einrichtungen und die durch die Richtlinie (EU) 2022/2555 eingesetzte Kooperationsgruppe sollten einen regelmäßigen Dialog aufnehmen, um die Zusammenarbeit zwischen den gemäß der vorliegenden Richtlinie und der Richtlinie (EU) 2022/2555 zuständigen Behörden zu fördern und den Informationsaustausch insbesondere zu Themen, die für beide Gruppen von Belang sind, zu erleichtern.

(39) Zur Verwirklichung der Ziele dieser Richtlinie und unbeschadet der rechtlichen Verantwortung der Mitgliedstaaten und der kritischen Einrichtungen, für die Erfüllung ihrer jeweiligen in der Richtlinie festgelegten Verpflichtungen zu sorgen, sollte die Kommission, sofern sie dies für angemessen hält, zuständige Behörden und kritische Einrichtungen unterstützen, um diesen die Erfüllung ihrer entsprechenden Verpflichtungen zu erleichtern. Bei der Unterstützung der Mitgliedstaaten und kritischen Einrichtungen bei der Umsetzung der Verpflichtungen aus dieser Richtlinie sollte die Kommission auf bestehenden Strukturen und Instrumenten aufbauen, beispielsweise auf denjenigen im Rahmen des mit dem Beschluss Nr. 1313/2013/EU eingerichteten Katastrophenschutzverfahrens der Union und dem Europäischen Referenznetz für den Schutz kritischer Infrastrukturen. Darüber hinaus sollte sie die Mitgliedstaaten über die Ressourcen unterrichten, die auf Unionsebene verfügbar sind, wie etwa im Rahmen des durch die Verordnung (EU) 2021/1149 des Europäischen Parlaments und des Rates ([23]) eingerichteten Fonds für die innere Sicherheit, des durch die Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates ([24]) eingerichteten Programms „Horizont Europa“ oder anderer für die Resilienz kritischer Einrichtungen relevanter Instrumente.

(40) Die Mitgliedstaaten sollten dafür sorgen, dass ihre zuständigen Behörden über bestimmte spezifische Befugnisse für die ordnungsgemäße Anwendung und Durchsetzung dieser Richtlinie in Bezug auf kritische Einrichtungen verfügen, die gemäß dieser Richtlinie ihrer rechtlichen Zuständigkeit unterliegen. Diese Befugnisse sollten insbesondere die Möglichkeit umfassen, Inspektionen und Audits durchzuführen, Aufsichtsmaßnahmen durchzuführen, kritische Einrichtungen dazu zu verpflichten, Informationen und Nachweise über die Maßnahmen vorzulegen, die sie zur Erfüllung ihrer Verpflichtungen ergriffen haben, und erforderlichenfalls Anordnungen zur Behebung festgestellter Verstöße zu erlassen. Beim Erlass solcher Anordnungen sollten die Mitgliedstaaten keine Maßnahmen vorschreiben, die über das hinausgehen, was erforderlich und verhältnismäßig ist, um die Erfüllung der jeweiligen Verpflichtung durch die betreffende kritische Einrichtung sicherzustellen, wobei insbesondere der Schwere des Verstoßes und der wirtschaftlichen Leistungsfähigkeit der betreffenden kritischen Einrichtung Rechnung zu tragen ist. Generell sollten diese Befugnisse mit angemessenen und wirksamen Garantien einhergehen,

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

([23]) Verordnung (EU) 2021/1149 des Europäischen Parlaments und des Rates vom 7. Juli 2021 zur Einrichtung des Fonds für die innere Sicherheit (ABl. L 251 vom 15.7.2021, S. 94).

([24]) Verordnung (EU) 2021/695 des Europäischen Parlaments und des Rates vom 28. April 2021 zur Einrichtung von „Horizont Europa“, dem Rahmenprogramm für Forschung und Innovation, sowie über dessen Regeln für die Beteiligung und die Verbreitung der Ergebnisse und zur Aufhebung der Verordnungen (EU) Nr. 1290/2013 und (EU) Nr. 1291/2013 (ABl. L 170 vom 12.5.2021, S. 1).

die im nationalen Recht im Einklang mit der Charta der Grundrechte der Europäischen Union festzulegen sind. Im Zuge der Bewertung, ob eine kritische Einrichtung ihre, in dieser Richtlinie festgelegten Verpflichtungen erfüllt, sollten die nach der vorliegenden Richtlinie zuständigen Behörden die gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden ersuchen können, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine in den Anwendungsbereich jener Richtlinie fallende Einrichtung auszuüben, die gemäß der vorliegenden Richtlinie als eine kritische Einrichtung eingestuft wurde. Die gemäß der vorliegenden Richtlinie zuständigen Behörden und die gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden sollten zu diesem Zweck zusammenarbeiten und Informationen austauschen.

(41) Um diese Richtlinie wirksam und kohärent anzuwenden, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 AEUV Rechtsakte zur Ergänzung dieser Richtlinie durch die Erstellung einer Liste der wesentlichen Dienste zu erlassen. Diese Liste sollte von den zuständigen Behörden für die Zwecke der Durchführung von Risikobewertungen durch Mitgliedstaaten und für die Ermittlung kritischer Einrichtungen gemäß dieser Richtlinie verwendet werden. In Anbetracht des in dieser Richtlinie verfolgten Ansatzes der Mindestharmonisierung ist diese Liste nicht erschöpfend, und die Mitgliedstaaten könnten sie durch zusätzliche wesentliche Dienste auf nationaler Ebene ergänzen, um nationalen Besonderheiten bei der Erbringung wesentlicher Dienste Rechnung zu tragen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([25]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(42) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Richtlinie sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten im Einklang mit der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([26]) ausgeübt werden.

(43) Da die Ziele dieser Richtlinie, nämlich die Gewährleistung der Erbringung von Diensten im Binnenmarkt, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten von wesentlicher Bedeutung sind, und die Verbesserung der Resilienz der diese Dienste erbringenden kritischen Einrichtungen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen der Wirkung der Maßnahme auf Unionsebene besser zu verwirklichen sind, kann die Union im 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 dieser Ziele erforderliche Maß hinaus.

(44) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([27]) angehört und hat am 11. August 2021 eine Stellungnahme abgegeben.

(45) Die Richtlinie 2008/114/EG sollte daher aufgehoben werden —

([25]) ABl. L 123 vom 12.5.2016, S. 1.

([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).

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

HABEN FOLGENDE RICHTLINIE ERLASSEN:

KAPITEL I

**ALLGEMEINE BESTIMMUNGEN**

*Artikel 1*

**Gegenstand und Anwendungsbereich**

(1) Die vorliegende Richtlinie

a) legt Verpflichtungen gegenüber Mitgliedstaaten fest zur Gewährleistung der ungehinderten Erbringung von Diensten im Binnenmarkt, die für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen oder wirtschaftlicher Tätigkeiten unerlässlich sind, spezifische Maßnahmen im Sinne von Artikel 114 AEUV zu ergreifen, und insbesondere Verpflichtungen kritische Einrichtungen zu ermitteln und diese kritischen Einrichtungen dabei zu unterstützen, die ihnen auferlegten Verpflichtungen zu erfüllen;

b) legt Verpflichtungen für kritische Einrichtungen fest, die darauf abzielen, ihre Resilienz und ihre Fähigkeit zur Erbringung von Diensten gemäß Buchstabe a im Binnenmarkt zu verbessern;

c) legt Vorschriften fest im Hinblick auf

   i) die Beaufsichtigung kritischer Einrichtungen

   ii) die Durchsetzungsmaßnahmen;

   iii) die Ermittlung kritischer Einrichtungen, die für Europa von besonderer Bedeutung sind, und die Beratungsmissionen zur Bewertung der Maßnahmen, die diese kritischen Einrichtungen ergriffen haben, um deren Verpflichtungen gemäß Kapitel III nachzukommen;

d) legt gemeinsame Verfahren für die Zusammenarbeit und die Berichterstattung über die Anwendung dieser Richtlinie fest;

e) legt Maßnahmen fest, mit denen ein hohes Maß an Resilienz kritischer Einrichtungen erreicht werden soll, um die Erbringung wesentlicher Dienste in der Union sicherzustellen und das Funktionieren des Binnenmarkts zu verbessern.

(2) Unbeschadet des Artikels 8 der vorliegenden Richtlinie gilt diese Richtlinie nicht für Angelegenheiten, die unter die Richtlinie (EU) 2022/2555 fallen. Angesichts der Beziehung zwischen physischer Sicherheit und Cybersicherheit kritischer Einrichtungen gewährleisten die Mitgliedstaaten eine koordinierte Umsetzung der vorliegenden Richtlinie und der Richtlinie (EU) 2022/2555.

(3) Wenn kritische Einrichtungen gemäß den Bestimmungen sektorspezifischer Rechtsakte der Union Maßnahmen zur Verbesserung ihrer Resilienz ergreifen müssen und diese Anforderungen von den Mitgliedstaaten den entsprechenden Verpflichtungen aus dieser Richtlinie als zumindest gleichwertig anerkannt sind, finden die entsprechenden Bestimmungen dieser Richtlinie, einschließlich der in Kapitel VI festgelegten Bestimmungen über Aufsicht und Durchsetzung, keine Anwendung.

(4) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union oder der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen entsprechenden Behörden in Übereinstimmung 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. Bei diesem Informationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen kritischer Einrichtungen unter Beachtung der Sicherheit der Mitgliedstaaten geschützt.

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

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

(7) Die Mitgliedstaaten können beschließen, dass Artikel 11 und die Kapitel III, IV und VI, ganz oder teilweise, keine Anwendung finden für spezifische kritische Einrichtungen, die Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung — einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten — ausüben oder Dienste ausschließlich für die in Absatz 6 des vorliegenden Artikels genannten Einrichtungen der öffentlichen Verwaltung erbringen.

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

(9) Das Unionsrecht betreffend den Schutz personenbezogener Daten, insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([28]) und die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([29]), bleibt von dieser Richtlinie unberührt.

*Artikel 2*

**Begriffsbestimmungen**

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „kritische Einrichtung“ eine öffentliche oder private Einrichtung, die ein Mitgliedstaat in Anwendung des Artikels 6 als einer der Kategorien in der dritten Spalte der Tabelle im Anhang angehörend eingestuft hat;

2. „Resilienz“ die Fähigkeit einer kritischen Einrichtung, einen Sicherheitsvorfall zu verhindern, sich davor zu schützen, darauf zu reagieren, einen solchen abzuwehren, die Folgen eines solchen Vorfalls zu begrenzen, einen Sicherheitsvorfall aufzufangen, zu bewältigen und sich von einem solchen Vorfall zu erholen;

3. „Sicherheitsvorfall“ ein Ereignis, das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte, einschließlich einer Beeinträchtigung der nationalen Systeme zur Wahrung der Rechtsstaatlichkeit;

4. „kritische Infrastrukturen“ Objekte, Anlagen, Ausrüstung, Netze oder Systeme oder Teile eines Objekts, einer Anlage, Ausrüstung, eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes erforderlich sind;

5. „wesentlicher Dienst“ einen Dienst, der für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder der Erhaltung der Umwelt von entscheidender Bedeutung ist;

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

7. „Risikobewertung“ den gesamten Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos, bei dem potenzielle entsprechende Bedrohungen, Schwachstellen und Gefahren, die zu einem Sicherheitsvorfall führen könnten, ermittelt und analysiert und die durch den Sicherheitsvorfall verursachten potenziellen Verluste oder Störungen bei der Erbringung eines wesentlichen Dienstes bewertet werden;

8. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([30]);

([28]) 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).

([29]) 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).

([30]) 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).

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

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

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

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

    c) sie wird überwiegend von staatlichen Behörden oder von anderen auf zentraler Ebene angesiedelten Körperschaften des öffentlichen Rechts finanziert, untersteht hinsichtlich ihrer Leitung der Aufsicht dieser Behörden oder Einrichtungen, oder sie hat ein Verwaltungs-, Leitungs- bzw. Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die von staatlichen Behörden oder von anderen auf zentraler Ebene angesiedelten 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.

*Artikel 3*

**Mindestharmonisierung**

Diese Richtlinie hindert die Mitgliedstaaten nicht daran, Bestimmungen des nationalen Rechts zur Erreichung eines höheren Resilienzniveaus für kritische Einrichtungen zu erlassen oder beizubehalten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen.

KAPITEL II

**NATIONALE RAHMEN FÜR DIE RESILIENZ KRITISCHER EINRICHTUNGEN**

*Artikel 4*

**Strategien für die Resilienz kritischer Einrichtungen**

(1) Nach einer Konsultation, die — soweit praktisch möglich — den entsprechenden Interessenvertretern offensteht, verabschiedet jeder Mitgliedstaat spätestens am 17. Januar 2026 eine Strategie zur Verbesserung der Resilienz kritischer Einrichtungen (im Folgenden „Strategie“). In der Strategie sind — aufbauend auf den bestehenden entsprechenden nationalen und sektorspezifischen Strategien, Plänen oder ähnlichen Dokumenten — die strategischen Ziele und politischen Maßnahmen festgelegt, mit denen ein hohes Resilienzniveau von kritischen Einrichtungen erreicht und aufrechterhalten werden soll und mindestens die im Anhang festgelegten Sektoren abgedeckt werden sollen.

(2) Jede Strategie enthält mindestens folgende Elemente:

a) strategische Ziele und Prioritäten zur Verbesserung der Gesamtresilienz kritischer Einrichtungen unter Berücksichtigung grenzüberschreitender und sektorübergreifender Abhängigkeiten und gegenseitiger Abhängigkeiten;

b) einen Steuerungsrahmen zur Verwirklichung der strategischen Ziele und Prioritäten, einschließlich einer Beschreibung der Aufgaben und Zuständigkeiten der jeweiligen Behörden, kritischen Einrichtungen und sonstigen an der Umsetzung der Strategie beteiligten Akteure;

c) eine Beschreibung der Maßnahmen, die zur Verbesserung der Gesamtresilienz kritischer Einrichtungen erforderlich sind, einschließlich einer Beschreibung der Risikobewertung nach Artikel 5;

d) eine Beschreibung des Verfahrens zur Ermittlung kritischer Einrichtungen;

e) eine Beschreibung des Prozesses zur Unterstützung kritischer Einrichtungen gemäß diesem Kapitel, einschließlich Maßnahmen zur Verbesserung der Zusammenarbeit zwischen dem öffentlichen Sektor einerseits und dem privaten Sektor und öffentlichen und privaten Einrichtungen andererseits;

f) eine Liste der wichtigsten Behörden und entsprechenden Interessenvertretern — bei denen es sich nicht um kritische Einrichtungen handelt —, die an der Umsetzung der Strategie beteiligt sind;

g) einen politischen Rahmen für die Koordinierung zwischen den gemäß der vorliegenden Richtlinie zuständigen Behörden (im Folgenden „zuständige Behörden") und den gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden für die Zwecke des Informationsaustauschs über Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle und über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle sowie die Wahrnehmung von Aufsichtsaufgaben;

h) eine Beschreibung der bereits bestehenden Maßnahmen zur Erleichterung der Umsetzung von Verpflichtungen gemäß Kapitel III der vorliegenden Richtlinie durch kleine und mittlere Unternehmen im Sinne des Anhangs der Empfehlung 2003/361/EG der Kommission ([31]), die von den betreffenden Mitgliedstaaten als kritische Einrichtungen eingestuft wurden.

Nach einer Konsultation, die — soweit praktisch möglich — den entsprechenden Interessenvertretern offensteht, aktualisieren die Mitgliedstaaten ihre Strategien mindestens alle vier Jahre.

(3) Die Mitgliedstaaten teilen der Kommission ihre Strategien und deren wesentlichen Aktualisierungen innerhalb von drei Monaten nach ihrer Verabschiedung mit.

*Artikel 5*

**Risikobewertung durch die Mitgliedstaaten**

(1) Der Kommission wird die Befugnis übertragen, bis zum 17. November 2023 delegierte Rechtsakte nach Artikel 23 zu erlassen, um diese Richtlinie durch eine nicht erschöpfende Liste wesentlicher Dienste in den im Anhang genannten Sektoren und Teilsektoren zu ergänzen. Die zuständigen Behörden verwenden jene Liste wesentlicher Dienste für die Zwecke einer Risikobewertung (im Folgenden „Risikobewertung durch Mitgliedstaaten"), die bis zum 17. Januar 2026 je nach Bedarf, mindestens aber alle vier Jahre, durchgeführt wird. Die zuständigen Behörden verwenden Risikobewertungen durch Mitgliedstaaten, um kritische Einrichtungen gemäß Artikel 6 zu ermitteln und diese bei der Ergreifung von Maßnahmen gemäß Artikel 13 zu unterstützen.

Bei Risikobewertungen durch Mitgliedstaaten werden die entsprechenden natürlichen und vom Menschen verursachten Risiken berücksichtigt, darunter solche sektorübergreifender oder grenzüberschreitender Art, Unfälle, Naturkatastrophen, gesundheitliche Notlagen, sowie hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([32]).

(2) Bei der Durchführung von Risikobewertungen durch Mitgliedstaaten berücksichtigen die Mitgliedstaaten mindestens

a) die nach Artikel 6 Absatz 1 des Beschlusses Nr. 1313/2013/EU vorgenommene allgemeine Risikobewertung;

b) sonstige entsprechende Risikobewertungen, die im Einklang mit den Anforderungen der entsprechenden sektorspezifischen Rechtsakte der Union, einschließlich der Verordnungen (EU) 2017/1938 ([33]) und (EU) 2019/941 ([34]) des Europäischen Parlaments und des Rates sowie der Richtlinien 2007/60/EG ([35]) und 2012/18/EU ([36]) des Europäischen Parlaments und des Rates, durchgeführt werden;

([31]) 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).

([32]) Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. L 88 vom 31.3.2017, S. 6).

([33]) Verordnung (EU) 2017/1938 des Europäischen Parlaments und des Rates vom 25. Oktober 2017 über Maßnahmen zur Gewährleistung der sicheren Gasversorgung und zur Aufhebung der Verordnung (EU) Nr. 994/2010 (ABl. L 280 vom 28.10.2017, S. 1).

([34]) Verordnung (EU) 2019/941 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über die Risikovorsorge im Elektrizitätssektor und zur Aufhebung der Richtlinie 2005/89/EG (ABl. L 158 vom 14.6.2019, S. 1).

([35]) Richtlinie 2007/60/EG des Europäischen Parlaments und des Rates vom 23. Oktober 2007 über die Bewertung und das Management von Hochwasserrisiken (ABl. L 288 vom 6.11.2007, S. 27).

([36]) Richtlinie 2012/18/EU des Europäischen Parlaments und des Rates vom 4. Juli 2012 zur Beherrschung der Gefahren schwerer Unfälle mit gefährlichen Stoffen, zur Änderung und anschließenden Aufhebung der Richtlinie 96/82/EG des Rates (ABl. L 197 vom 24.7.2012, S. 1).

c) die entsprechenden Risiken, die sich aus dem Ausmaß der Abhängigkeit zwischen den im Anhang genannten Sektoren, einschließlich dem Ausmaß der Abhängigkeit gegenüber in anderen Mitgliedstaaten und Drittstaaten ansässigen Einrichtungen, ergeben, sowie die Auswirkungen, die eine in einem Sektor auftretende erhebliche Störung auf andere Sektoren haben kann, darunter alle wesentlichen Risiken für die Bürger und Bürgerinnen und den Binnenmarkt;

d) sämtliche gemäß Artikel 15 gemeldeten Informationen über Sicherheitsvorfälle.

Für die Zwecke von Unterabsatz 1 Buchstabe c arbeiten die Mitgliedstaaten mit den zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit den zuständigen Behörden aus Drittstaaten zusammen.

(3) Die Mitgliedstaaten stellen die entsprechenden Elemente der Risikobewertungen durch Mitgliedstaaten den kritischen Einrichtungen, die sie gemäß Artikel 6 ermittelt haben, gegebenenfalls über ihre zentralen Anlaufstellen, zur Verfügung. Die Mitgliedstaaten stellen sicher, dass die den kritischen Einrichtungen zur Verfügung gestellten Informationen ihnen bei der Durchführung ihrer Risikobewertungen gemäß Artikel 12 und beim Ergreifen von Maßnahmen zur Gewährleistung ihrer Resilienz gemäß Artikel 13 unterstützen.

(4) Innerhalb von drei Monaten nach Durchführung einer Risikobewertung durch Mitgliedstaaten übermittelt ein Mitgliedstaat der Kommission entsprechende Informationen über die ermittelten Arten von Risiken und die Ergebnisse dieser Risikobewertungen durch Mitgliedstaaten, aufgeschlüsselt nach den im Anhang genannten Sektoren und Teilsektoren.

(5) Zum Zwecke der Einhaltung des Absatzes 4 arbeitet die Kommission in Zusammenarbeit mit den Mitgliedstaaten ein unverbindliches gemeinsames Berichtsmuster aus.

*Artikel 6*

**Ermittlung kritischer Einrichtungen**

(1) Bis zum 17. Juli 2026 ermittelt jeder Mitgliedstaat die kritischen Einrichtungen für die im Anhang festgelegten Sektoren und Teilsektoren.

(2) Wenn ein Mitgliedstaat kritische Einrichtungen gemäß Absatz 1 ermittelt, berücksichtigt er die Ergebnisse seiner Risikobewertung durch Mitgliedstaaten und seine Strategie und wendet alle folgenden Kriterien an:

a) Die Einrichtung erbringt einen oder mehrere wesentliche Dienste,

b) die Einrichtung ist im Hoheitsgebiet dieses Mitgliedstaats tätig und ihre kritische Infrastruktur befinden sich dort, und

c) ein Sicherheitsvorfall würde eine erhebliche Störung im Sinne von Artikel 7 Absatz 1 bei der Erbringung eines oder mehrerer wesentlichen Dienste durch die Einrichtung, oder bei der Erbringung von anderen wesentlichen Diensten in den im Anhang genannten Sektoren, die von diesem oder diesen wesentlichen Diensten abhängen, bewirken.

(3) Jeder Mitgliedstaat erstellt eine Liste der gemäß Absatz 2 ermittelten kritischen Einrichtungen und stellt sicher, dass diesen kritischen Einrichtungen innerhalb eines Monats nach der entsprechenden Ermittlung ihre Einstufung als kritische Einrichtung mitgeteilt wird. Unbeschadet des Artikels 8 informieren die Mitgliedstaaten diese kritischen Einrichtungen über ihre Verpflichtungen nach Kapiteln III und IV sowie über den Zeitpunkt, ab dem diese Verpflichtungen auf sie Anwendung finden. Die Mitgliedstaaten informieren die kritischen Einrichtungen in den in den Nummern 3, 4 und 8 der Tabelle des Anhangs genannten Sektoren darüber, dass sie keine Verpflichtungen nach Kapiteln III und IV haben, es sei denn, in den nationalen Maßnahmen ist etwas anderes bestimmt.

Für die betreffenden kritischen Einrichtungen gilt Kapitel III nach Ablauf von zehn Monaten ab dem Zeitpunkt der in Unterabsatz 1 des vorliegenden Absatzes genannten Mitteilung.

(4) Die Mitgliedstaaten stellen sicher, dass ihre nach dieser Richtlinie zuständigen Behörden den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 innerhalb eines Monats nach der entsprechenden Einstufung die Identität der kritischen Einrichtungen mitteilen, die sie gemäß diesem Artikel ermittelt haben. In dieser Mitteilung wird gegebenenfalls angegeben, dass es sich bei den betreffenden kritischen Einrichtungen um Einrichtungen in den in den Nummern 3, 4 und 8 der Tabelle des Anhangs der vorliegenden Richtlinie genannten Sektoren handelt und dass sie keine Verpflichtungen nach den Kapiteln III und IV haben.

(5) Die Mitgliedstaaten überprüfen die in Absatz 3 genannten Liste der ermittelten kritischen Einrichtungen im Bedarfsfall, mindestens jedoch alle vier Jahre, und aktualisieren sie gegebenenfalls. Führen diese Aktualisierungen zur Ermittlung weiterer kritischer Einrichtungen, so gelten die Absätze 3 und 4 für diese zusätzlichen kritischen Einrichtungen. Darüber hinaus stellen die Mitgliedstaaten sicher, dass Einrichtungen, die nach einer solchen Aktualisierung nicht mehr als kritische Einrichtung eingestuft werden, hiervon rechtzeitig in Kenntnis gesetzt und darüber informiert werden, dass sie ab dem Tag des Erhalts dieser Mitteilung nicht mehr den Verpflichtungen nach Kapitel III unterliegen.

(6) Die Kommission arbeitet in Zusammenarbeit mit den Mitgliedstaaten Empfehlungen und unverbindliche Leitlinien aus, um die Mitgliedstaaten bei der Ermittlung kritischer Einrichtungen zu unterstützen.

*Artikel 7*

**Erhebliche Störung**

(1) Bei der Bestimmung des Ausmaßes einer Störung gemäß Artikel 6 Absatz 2 Buchstabe c berücksichtigen die Mitgliedstaaten die folgenden Kriterien:

a) die Zahl der Nutzer, die den von der betreffenden Einrichtung erbrachten wesentlichen Dienst in Anspruch nehmen;

b) das Ausmaß der Abhängigkeit anderer im Anhang festgelegten Sektoren und Teilsektoren von dem betreffenden wesentlichen Dienst;

c) die möglichen Auswirkungen von Sicherheitsvorfällen — hinsichtlich Ausmaß und Dauer — auf wirtschaftliche und gesellschaftliche Tätigkeiten, die Umwelt, die öffentliche Ordnung und Sicherheit oder die Gesundheit der Bevölkerung;

d) den Marktanteil der Einrichtung auf dem Markt für wesentliche Dienste oder für die betreffenden wesentlichen Dienste;

e) das geografische Gebiet, das von einem Sicherheitsvorfall betroffen sein könnte, einschließlich etwaiger grenzüberschreitender Auswirkungen, unter Berücksichtigung der Schwachstellen, die mit dem Grad der Isolierung bestimmter Arten geografischer Gebiete — zum Beispiel Inselregionen, abgelegene Regionen oder Berggebiete — verbunden sind;

f) die Bedeutung der Einrichtung für die Aufrechterhaltung des wesentlichen Dienstes in ausreichendem Umfang, unter Berücksichtigung der Verfügbarkeit von alternativen Mitteln für die Erbringung des betreffenden wesentlichen Dienstes.

(2) Nach der Ermittlung der kritischen Einrichtungen gemäß Artikel 6 Absatz 1 übermittelt jeder Mitgliedstaat der Kommission unverzüglich folgende Informationen:

a) die Liste der wesentlichen Dienste in jenem Mitgliedstaat, wenn es dort zusätzliche wesentliche Dienste im Vergleich zu der in Artikel 5 Absatz 1 genannten Liste wesentlicher Dienste gibt,

b) die Zahl der ermittelten kritischen Einrichtungen für jeden im Anhang festgelegten Sektor und Teilsektor und für jeden wesentlichen Dienst,

c) alle Schwellenwerte, die zur Spezifizierung eines oder mehrerer der in Absatz 1 genannten Kriterien angewandt werden.

In Unterabsatz 1 Buchstabe c genannte Schwellenwerte können als solche oder in aggregierter Form dargestellt werden.

Anschließend übermitteln die Mitgliedstaaten Informationen gemäß Unterabsatz 1 im Bedarfsfall, mindestens jedoch alle vier Jahre.

(3) Die Kommission nimmt nach Konsultation der Gruppe für die Resilienz kritischer Einrichtungen gemäß Artikel 19 unter Berücksichtigung der in Absatz 2 des vorliegenden Artikels genannten Informationen unverbindliche Leitlinien an, um die Anwendung der in Absatz 1 des vorliegenden Artikels genannten Kriterien zu erleichtern.

*Artikel 8*

**Kritische Einrichtungen in den Sektoren Banken, Finanzmarktinfrastruktur und digitale Infrastruktur**

Die Mitgliedstaaten stellen sicher, dass Artikel 11 und die Kapitel III, IV und VI nicht für die von ihnen ermittelten kritischen Einrichtungen in den Sektoren gelten, die unter den Nummern 3, 4 und 8 in der Tabelle im Anhang aufgeführt sind. Die Mitgliedstaaten können nationale Vorschriften erlassen oder beibehalten, um ein höheres Maß an Resilienz für diese kritischen Einrichtungen zu erreichen, sofern diese Vorschriften mit dem geltenden Unionsrecht vereinbar sind.

*Artikel 9*

**Zuständige Behörden und zentrale Anlaufstelle**

(1) Jeder Mitgliedstaat benennt eine oder mehrere zuständige Behörden oder richtet diese ein, die für die ordnungsgemäße Anwendung und erforderlichenfalls Durchsetzung der in dieser Richtlinie festgelegten Vorschriften auf nationaler Ebene verantwortlich sind.

In Bezug auf die kritischen Einrichtungen in den Sektoren, die unter den Nummern 3 und 4 in der Tabelle im Anhang dieser Richtlinie festgelegt sind, sind die zuständigen Behörden grundsätzlich die in Artikel 46 der Verordnung (EU) 2022/2554 genannten zuständigen Behörden. In Bezug auf die kritischen Einrichtungen in den Sektoren, die unter der Nummer 8 in der Tabelle im Anhang dieser Richtlinie festgelegt sind, sind die zuständigen Behörden grundsätzlich die zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555. Die Mitgliedstaaten können im Einklang mit den bestehenden nationalen Rahmen eine andere zuständige Behörde für die in den Absätzen 3, 4 und 8 der im Anhang der vorliegenden Richtlinie festgelegten Tabelle aufgeführten Sektoren benennen.

Benennen die Mitgliedstaaten mehr als eine zuständige Behörde oder richten mehr als eine ein, so legen sie die Aufgaben jeder der betreffenden Behörden eindeutig fest und stellen sicher, dass diese wirksam zusammenarbeiten, um ihre Aufgaben im Rahmen dieser Richtlinie, unter anderem in Bezug auf die Benennung und die Tätigkeiten der zentralen Anlaufstelle gemäß Absatz 2, zu erfüllen.

(2) Jeder Mitgliedstaat sorgt für die Benennung oder Errichtung einer einzigen zentralen Anlaufstelle, die als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit mit den zentralen Anlaufstellen anderer Mitgliedstaaten und mit der in Artikel 19 genannten Gruppe für die Resilienz kritischer Einrichtungen (im Folgenden „zentrale Anlaufstelle“) fungiert. Gegebenenfalls benennt ein Mitgliedstaat seine zentrale Anlaufstelle innerhalb einer zuständigen Behörde. Gegebenenfalls kann ein Mitgliedstaat vorsehen, dass seine zentrale Anlaufstelle auch als Verbindungsstelle zur Kommission fungiert und die Zusammenarbeit mit Drittländern gewährleistet.

(3) Bis zum 17. Juli 2028 und danach alle zwei Jahre legen die zentralen Anlaufstellen der Kommission und der gemäß Artikel 19 genannten Gruppe für die Resilienz kritischer Einrichtungen einen zusammenfassenden Bericht über die bei ihnen eingegangenen Meldungen, einschließlich der Zahl der Meldungen, der Art der gemeldeten Sicherheitsvorfälle und der gemäß Artikel 15 Absatz 3 ergriffenen Maßnahmen, vor.

Die Kommission arbeitet in Zusammenarbeit mit der Gruppe für die Resilienz kritischer Einrichtungen ein gemeinsames Berichtsmuster aus. Die zuständigen Behörden können auf freiwilliger Basis dieses gemeinsame Berichtsmuster für die Vorlage der zusammenfassenden Berichte gemäß Unterabsatz 1 verwenden.

(4) Jeder Mitgliedstaat stellt sicher, dass seine zuständige Behörde und zentrale Anlaufstelle über die erforderlichen Befugnisse und angemessene finanzielle, personelle und technische Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient zu erfüllen.

(5) Jeder Mitgliedstaat stellt sicher, dass seine zuständige Behörde im Einklang mit dem Unionsrecht und dem nationalen Recht gegebenenfalls andere entsprechende nationale Behörden, unter anderem diejenigen, die für den Katastrophenschutz, die Strafverfolgung und den Schutz personenbezogener Daten zuständig ist, sowie kritische Einrichtungen und entsprechende interessierte Parteien konsultiert und mit ihnen zusammenarbeitet.

(6) Jeder Mitgliedstaat stellt sicher, dass seine nach dieser Richtlinie zuständige Behörde mit den nach Richtlinie (EU) 2022/2555 zuständigen Behörden in Bezug auf Cybersicherheitsrisiken, Cyberbedrohungen und Cybersicherheitsvorfälle und in Bezug auf nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle, die kritische Einrichtungen betreffen, sowie in Bezug auf entsprechende Maßnahmen, die von seiner zuständigen Behörde und den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 ergriffen wurden, zusammenarbeitet und Informationen austauscht.

(7) Innerhalb von drei Monaten nach der Benennung oder Errichtung der zuständigen Behörde und der zentralen Anlaufstelle, setzt jeder Mitgliedstaat die Kommission über deren Identität sowie deren Aufgaben und Zuständigkeiten gemäß dieser Richtlinie, deren Kontaktdaten und etwaiger späterer Änderungen dieser Angaben in Kenntnis. Mitgliedstaaten informieren die Kommission, wenn sie die Benennung einer anderen als der in Absatz 1 Unterabsatz 2 genannten Behörde als zuständige Behörde in Bezug auf kritischen Einrichtungen in den Sektoren, die unter den Nummern 3, 4 und 8 in der Tabelle im Anhang dieser Richtlinie festgelegt sind, beschließen. Jeder Mitgliedstaat gibt die Identität der zuständigen Behörde und der zentralen Anlaufstelle öffentlich bekannt.

(8) Die Kommission erstellt eine öffentlich verfügbare Liste der zentralen Anlaufstellen.

*Artikel 10*

**Unterstützung kritischer Einrichtungen durch die Mitgliedstaaten**

(1) Die Mitgliedstaaten unterstützen kritische Einrichtungen bei der Verbesserung ihrer Resilienz. Diese Unterstützung kann die Entwicklung von Leitfäden und Methoden, die Unterstützung der Organisation von Übungen zur Überprüfung ihrer Resilienz und die Bereitstellung von Beratung und Schulungen für Personal kritischer Einrichtungen umfassen. Die Mitgliedstaaten können kritischen Einrichtungen unbeschadet der geltenden Vorschriften für staatliche Beihilfen Finanzmittel zur Verfügung stellen, wenn dies erforderlich und durch im öffentlichen Interesse liegende Ziele gerechtfertigt ist.

(2) Jeder Mitgliedstaat stellt sicher, dass die zuständigen Behörden mit den kritischen Einrichtungen der im Anhang festgelegten Sektoren zusammenarbeiten sowie Informationen und bewährte Verfahren austauschen.

(3) Die Mitgliedstaaten erleichtern den freiwilligen Informationsaustausch zwischen kritischen Einrichtungen in unter diese Richtlinie fallenden Fragen im Einklang mit dem Unionsrecht und dem nationalen Recht, insbesondere in Fragen bezüglich Verschlusssachen und sensibler Informationen, des Wettbewerbs und des Schutzes personenbezogener Daten.

*Artikel 11*

**Zusammenarbeit zwischen Mitgliedstaaten**

(1) Die Mitgliedstaaten konsultieren einander gegebenenfalls in Bezug auf kritische Einrichtungen zur Sicherstellung der einheitlichen Anwendung dieser Richtlinie. Diese Konsultationen finden insbesondere in Bezug auf kritische Einrichtungen statt,

a) die kritische Infrastrukturen nutzen, die physisch zwischen zwei oder mehr Mitgliedstaaten verbunden sind,

b) die Teil von Unternehmensstrukturen sind, die mit kritischen Einrichtungen in anderen Mitgliedstaaten verbunden sind oder zu ihnen in Bezug stehen,

c) die als kritische Einrichtungen in einem Mitgliedstaat eingestuft wurden und wesentliche Dienste für andere bzw. in anderen Mitgliedstaaten erbringen.

(2) Ziel der Konsultationen nach Absatz 1 ist es, die Resilienz kritischer Einrichtungen zu verbessern und, soweit möglich, den Verwaltungsaufwand für diese zu verringern.

KAPITEL III

**RESILIENZ KRITISCHER EINRICHTUNGEN**

*Artikel 12*

**Risikobewertungen durch kritische Einrichtungen**

(1) Ungeachtet der in Artikel 6 Absatz 3 Unterabsatz 2 festgelegten Frist, stellen die Mitgliedstaaten sicher, dass kritische Einrichtungen innerhalb von neun Monaten nach Erhalt der in Artikel 6 Absatz 3 genannten Mitteilung und anschließend im Bedarfsfall, mindestens jedoch alle vier Jahre, eine Risikobewertung auf der Grundlage der Risikobewertungen durch Mitgliedstaaten und anderer entsprechender Informationsquellen durchführen, um alle entsprechenden Risiken zu bewerten, die die Erbringung ihrer wesentlichen Dienste (im Folgenden „Risikobewertung durch kritische Einrichtungen“) stören könnten.

(2) Die Risikobewertung durch kritische Einrichtungen trägt allen entsprechenden natürlichen und vom Menschen verursachten Risiken Rechnung, die zu einem Sicherheitsvorfall führen könnten, einschließlich grenzüberschreitender oder sektorübergreifender Risiken, Unfällen, Naturkatastrophen, gesundheitlicher Notlagen und hybriden Bedrohungen und anderen feindlichen Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541. Eine Risikobewertung durch kritische Einrichtungen trägt dem Ausmaß der Abhängigkeit anderer im Anhang festgelegten Sektoren von dem wesentlichen Dienst, der von der kritischen Einrichtung — gegebenenfalls auch in benachbarten Mitgliedstaaten und Drittländern — erbracht wird, und dem Ausmaß der Abhängigkeit der kritischen Einrichtung von den wesentlichen Diensten, der von anderen Einrichtungen in anderen Sektoren — gegebenenfalls auch in benachbarten Mitgliedstaaten und Drittländern — erbracht wird, Rechnung.

Hat eine kritische Einrichtung aufgrund von Verpflichtungen aus anderen Rechtsakten, die für ihre Risikobewertung durch kritische Einrichtungen relevant sind, andere Risikobewertungen vorgenommen oder Dokumente erstellt, so kann sie diese Bewertungen und Dokumente verwenden, um die in diesem Artikel festgelegten Anforderungen zu erfüllen. Bei der Wahrnehmung ihrer Aufsichtsaufgaben kann die zuständige Behörde eine bestehende Risikobewertung, die von einer kritischen Einrichtung durchgeführt wurde, die sich mit den in Unterabsatz 1 genannten Risiken und dem Ausmaß der Abhängigkeit befasst, als vollständig oder teilweise den Verpflichtungen nach diesem Artikel entsprechend erklären.

*Artikel 13*

**Resilienzmaßnahmen kritischer Einrichtungen**

(1) Die Mitgliedstaaten stellen sicher, dass die kritischen Einrichtungen auf der Grundlage der von den Mitgliedstaaten bereitgestellten entsprechenden Informationen über die Risikobewertung durch Mitgliedstaaten sowie den Ergebnissen der Risikobewertung durch kritische Einrichtungen geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz ergreifen, unter anderem Maßnahmen, die erforderlich sind, um

a) das Auftreten von Sicherheitsvorfällen zu verhindern, unter gebührender Berücksichtigung von Katastrophenvorsorge und Maßnahmen zur Anpassung an den Klimawandel;

b) einen angemessenen physischen Schutz ihrer Räumlichkeiten und kritischen Infrastrukturen zu gewährleisten, unter gebührender Berücksichtigung zum Beispiel von dem Aufstellen von Zäunen und Sperren, Instrumenten und Verfahren für die Überwachung der Umgebung, Detektionsgeräten und Zugangskontrollen;

c) auf Sicherheitsvorfälle zu reagieren, sie abzuwehren und die Folgen solcher Vorfälle zu begrenzen, unter gebührender Berücksichtigung der Umsetzung von Risiko- und Krisenmanagementverfahren und -protokollen und vorgegebener Abläufe im Alarmfall;

d) nach Sicherheitsvorfällen die Wiederherstellung zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen zur Aufrechterhaltung des Betriebs und der Ermittlung alternativer Lieferketten, um die Erbringung des wesentlichen Dienstes wiederaufzunehmen;

e) ein angemessenes Sicherheitsmanagement hinsichtlich der Mitarbeiter zu gewährleisten, unter gebührender Berücksichtigung von Maßnahmen wie der Festlegung von Kategorien von Personal, das kritische Funktionen wahrnimmt, der Festlegung von Zugangsrechten zu Räumlichkeiten, kritischen Infrastrukturen und zu sensiblen Informationen und der Einführung von Verfahren für Zuverlässigkeitsüberprüfungen im Einklang mit Artikel 14 und der Benennung von Kategorien von Personal, die solche Zuverlässigkeitsüberprüfungen durchlaufen müssen, und der Festlegung angemessener Schulungsanforderungen und Qualifikationen.

f) das entsprechende Personal für die unter den Buchstaben a bis e genannten Maßnahmen unter gebührender Berücksichtigung von Schulungen, Informationsmaterial und Übungen zu sensibilisieren.

Für die Zwecke von Unterabsatz 1 Buchstabe e stellen die Mitgliedstaaten sicher, dass kritische Einrichtungen das Personal externer Dienstleister bei der Festlegung der Kategorien von Personal, das kritische Funktionen wahrnimmt, berücksichtigt;

(2) Die Mitgliedstaaten stellen sicher, dass kritische Einrichtungen über einen Resilienzplan oder ein gleichwertiges Dokument oder Dokumente, in denen die Maßnahmen gemäß Absatz 1 beschrieben werden, verfügen und diese anwenden. Haben kritische Einrichtungen Dokumente erstellt oder Maßnahmen aufgrund von Verpflichtungen aus anderen Rechtsakten, die für die in Absatz 1 genannten Maßnahmen relevant sind, ergriffen, so können sie diese Dokumente und Maßnahmen verwenden, um die in diesem Artikel festgelegten Anforderungen zu erfüllen. Bei der Wahrnehmung ihrer Aufsichtsaufgaben kann die zuständige Behörde bestehende Maßnahmen zur Verbesserung der Resilienz einer kritischen Einrichtung, die die in Absatz 1 genannten technischen, sicherheitsbezogenen und organisatorischen Maßnahmen betreffen, als vollständig oder teilweise den Verpflichtungen nach diesem Artikel entsprechend erklären.

(3) Die Mitgliedstaaten stellen sicher, dass jede kritische Einrichtung einen Verbindungsbeauftragten oder eine Person mit vergleichbarer Aufgabenstellung als Ansprechpartner für die zuständigen Behörden benennt.

(4) Auf Ersuchen des Mitgliedstaats, der die kritische Einrichtung ermittelt hat, und mit Zustimmung der betreffenden kritischen Einrichtung organisiert die Kommission im Einklang mit den Regelungen gemäß Artikel 18 Absätze 6, 8 und 9 Beratungsmissionen, um die betreffende kritische Einrichtung im Hinblick auf die Erfüllung ihrer Verpflichtungen nach Kapitel III zu beraten. Die Beratungsmission erstattet der Kommission, dem betreffenden Mitgliedstaat und der betreffenden kritischen Einrichtung Bericht über ihre Ergebnisse.

(5) Die Kommission erlässt nach Konsultation der Gruppe für die Resilienz kritischer Einrichtungen gemäß Artikel 19 unverbindliche Leitlinien, in denen die technischen, sicherheitsbezogenen und organisatorischen Maßnahmen, die gemäß Absatz 1 des vorliegenden Artikels ergriffen werden können, näher spezifiziert werden.

(6) Die Kommission erlässt Durchführungsrechtsakte, um die erforderlichen technischen und methodischen Spezifikationen für die Anwendung der in Absatz 1 des vorliegenden Artikels genannten Maßnahmen festzulegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 24 Absatz 2 genannten Prüfverfahren erlassen.

*Artikel 14*

**Zuverlässigkeitsüberprüfungen**

(1) Die Mitgliedstaaten legen die Bedingungen fest, unter denen eine kritische Einrichtung in hinreichend begründeten Fällen und unter Berücksichtigung der Risikobewertung durch Mitgliedstaaten Anträge auf Zuverlässigkeitsüberprüfungen von Personen stellen darf, die

a) sensible Funktionen in oder zugunsten der kritischen Einrichtung innehaben, insbesondere in Bezug auf die Resilienz der kritischen Einrichtung;

b) berechtigt sind, über einen direkten Zugriff oder Fernzugriff auf ihre Räumlichkeiten, Informationen oder Kontrollsysteme zu verfügen, auch im Zusammenhang mit der Sicherheit der kritischen Einrichtung;

c) für die Besetzung von Positionen, die unter die in den Buchstaben a und b festgelegten Kriterien fallen, in Betracht gezogen werden.

(2) Anträge gemäß Absatz 1 des vorliegenden Artikels werden innerhalb eines angemessenen Zeitrahmens geprüft und im Einklang mit dem nationalen Recht und Verfahren sowie dem entsprechenden und geltenden Unionsrecht — einschließlich der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([37]) — bearbeitet. Zuverlässigkeitsüberprüfungen müssen verhältnismäßig und strikt auf das Notwendige beschränkt sein. Sie werden ausschließlich zum Zweck der Bewertung eines potenziellen Sicherheitsrisikos für die betreffende kritische Einrichtung durchgeführt.

(3) Eine in Absatz 1 genannte Zuverlässigkeitsüberprüfung muss mindestens

a) sich der Identität der Person, die einer Zuverlässigkeitsüberprüfung unterzogen wird, vergewissern;

b) eine Strafregisterprüfung der Person in Bezug auf Straftaten, die für eine spezifische Position relevant sind, enthalten.

Bei Zuverlässigkeitsüberprüfungen nutzen die Mitgliedstaaten das Europäische Strafregisterinformationssystem gemäß den im Rahmenbeschluss 2009/315/JI und — sofern relevant und anwendbar — in der Verordnung (EU) 2019/816 festgelegten Verfahren zur Einholung von Informationen aus den Strafregistern von anderen Mitgliedstaaten. Die in Artikel 3 Absatz 1 des Rahmenbeschlusses 2009/315/JI und Artikel 3 Nummer 5 der Verordnung (EU) 2019/816 genannten Zentralbehörden beantworten Ersuchen um solche Informationen im Einklang mit Artikel 8 Absatz 1 des Rahmenbeschlusses 2009/315/JI innerhalb von zehn Arbeitstagen nach Eingang des Ersuchens gemäß Artikel 8 Absatz 1 des Rahmenbeschlusses 2009/315/JI.

([37]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

*Artikel 15*

**Meldung von Sicherheitsvorfällen**

(1) Die Mitgliedstaaten stellen sicher, dass die kritischen Einrichtungen der zuständigen Behörde Sicherheitsvorfälle, die die Erbringung wesentlicher Dienste erheblich stören oder erheblich stören könnten, unverzüglich melden. Die Mitgliedstaaten stellen sicher, dass außer wenn dies in operativer Hinsicht nicht möglich ist, kritische Einrichtungen eine erste Meldung bis spätestens 24 Stunden, nachdem sie sich eines Sicherheitsvorfalls bewusst geworden sind, übermitteln, gegebenenfalls gefolgt von einem ausführlichen Bericht spätestens einen Monat danach. Zur Bestimmung der Erheblichkeit einer Störung werden insbesondere folgende Parameter berücksichtigt:

a) Anzahl und Anteil der von der Störung betroffenen Nutzer;

b) Dauer der Störung;

c) betroffenes geografisches Gebiet der Störung, unter Berücksichtigung des Umstandes, ob das Gebiet geografisch isoliert ist.

Hat ein Sicherheitsvorfall erhebliche Auswirkungen auf die Kontinuität der Erbringung wesentlicher Dienste für oder in sechs oder mehr Mitgliedstaaten oder könnte er solche Auswirkungen haben, so melden die zuständigen Behörden der vom Sicherheitsvorfall betroffenen Mitgliedstaaten diesen Sicherheitsvorfall der Kommission.

(2) Die Meldungen gemäß Absatz 1 Unterabsatz 1 müssen sämtliche verfügbaren Informationen enthalten, die erforderlich sind, damit die zuständige Behörde Art, Ursache und mögliche Folgen des Sicherheitsvorfalls nachvollziehen und ermitteln kann, einschließlich verfügbarer Informationen, die notwendig sind, um zu bestimmen, ob der Sicherheitsvorfall grenzüberschreitende Auswirkungen hat. Solche Meldungen begründen keine höhere Haftung der betreffenden kritischen Einrichtung.

(3) Auf der Grundlage der in einer Meldung gemäß Absatz 1 bereitgestellten Informationen der kritischen Einrichtung unterrichtet die entsprechende zuständige Behörde über die zentrale Anlaufstelle die zentralen Anlaufstellen anderer betroffener Mitgliedstaaten, sofern der Sicherheitsvorfall erhebliche Auswirkungen auf kritische Einrichtungen und die Aufrechterhaltung der Erbringung wesentlicher Dienste an einen oder mehrere andere Mitgliedstaaten oder in einem oder mehreren anderen Mitgliedstaaten hat oder haben könnte.

Zentrale Anlaufstellen, die Informationen gemäß Unterabsatz 1 senden und erhalten, behandeln im Einklang mit dem Unionsrecht oder mit dem nationalen Recht die Informationen so, dass ihre Vertraulichkeit gewahrt und die Sicherheit und die geschäftlichen Interessen der betreffenden kritischen Einrichtung geschützt werden.

(4) So bald wie möglich nach einer Meldung gemäß Absatz 1 übermittelt die betreffende zuständige Behörde der betreffenden kritischen Einrichtung sachdienliche Folgeinformationen, unter anderem Informationen, die die wirksame Reaktion dieser kritischen Einrichtung auf den betreffenden Sicherheitsvorfall unterstützen könnten. Die Mitgliedstaaten informieren die Öffentlichkeit, wenn sie zu der Ansicht gelangen, dass dies im öffentlichen Interesse liegen würde.

*Artikel 16*

**Normen**

Um die abgestimmte Umsetzung dieser Richtlinie voranzutreiben, fördern die Mitgliedstaaten die Anwendung von europäischen und internationalen Normen und technischen Spezifikationen, die für die Maßnahmen zur Sicherheit und Resilienz kritischer Einrichtungen relevant sind, sofern dies sinnvoll ist und ohne die Verwendung einer bestimmten Technologieart vorzuschreiben oder diese zu bevorzugen.

KAPITEL IV

## KRITISCHE EINRICHTUNGEN, DIE VON BESONDERER BEDEUTUNG FÜR EUROPA SIND

*Artikel 17*

### Ermittlung kritischer Einrichtungen, die von besonderer Bedeutung für Europa sind

(1) Eine Einrichtung gilt als kritische Einrichtung von besonderer Bedeutung für Europa, wenn sie

a) gemäß Artikel 6 Absatz 1 als kritische Einrichtung eingestuft wurde,

b) für bzw. in sechs oder mehr Mitgliedstaaten dieselben oder ähnliche wesentliche Dienste erbringt und

c) gemäß Absatz 3 dieses Artikels gemeldet wurde.

(2) Die Mitgliedstaaten stellen sicher, dass eine kritische Einrichtung nach der Mitteilung gemäß Artikel 6 Absatz 3 ihre zuständige Behörde informiert, wenn sie wesentliche Dienste für bzw. in sechs oder mehr Mitgliedstaaten erbringt. Wenn dies der Fall ist, stellen die Mitgliedstaaten sicher, dass die kritische Einrichtung ihre zuständige Behörde darüber informiert welche wesentlichen Dienste sie für bzw. in diesen Mitgliedstaaten anbietet und für welche bzw. in welchen Mitgliedstaaten sie diese anbietet. Die Mitgliedstaaten teilen der Kommission unverzüglich die Identität solcher kritischen Einrichtungen sowie die Informationen, die diese gemäß dieses Absatzes zur Verfügung stellen, mit.

Die Kommission konsultiert die zuständige Behörde des Mitgliedstaats, der eine kritische Einrichtung gemäß Unterabsatz 1 ermittelt hat, die zuständige Behörde anderer betroffener Mitgliedstaaten sowie die betreffende kritische Einrichtung. Bei diesen Konsultationen teilt jeder Mitgliedstaat der Kommission mit, ob es sich seiner Einschätzung nach bei den Diensten, die diesem Mitgliedstaat von der kritischen Einrichtung erbracht werden, um wesentliche Dienste handelt.

(3) Stellt die Kommission auf der Grundlage der Konsultationen nach Absatz 2 fest, dass die betreffende kritische Einrichtung für bzw. in sechs oder mehr Mitgliedstaaten wesentliche Dienste erbringt, so teilt die Kommission dieser kritischen Einrichtung über deren zuständige Behörde mit, dass sie als kritische Einrichtung von besonderer Bedeutung für Europa gilt, und unterrichtet diese kritische Einrichtung über ihre Verpflichtungen gemäß diesem Kapitel sowie über den Zeitpunkt, ab dem diese Verpflichtungen für sie gelten. Sobald die Kommission die zuständige Behörde über ihre Entscheidung informiert, eine Einrichtung als kritische Einrichtung von besonderer Bedeutung für Europa zu betrachten, leitet die zuständige Behörde diese Meldung unverzüglich an diese kritische Einrichtung weiter.

(4) Dieses Kapitel gilt für die betreffende kritische Einrichtung von besonderer Bedeutung für Europa ab dem Tag des Eingangs der in Absatz 3 genannten Mitteilung.

*Artikel 18*

### Beratungsmissionen

(1) Auf Antrag eines Mitgliedstaats, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, organisiert die Kommission eine Beratungsmission zur Bewertung der Maßnahmen, die jene kritische Einrichtung ergriffen hat, um ihren Verpflichtungen gemäß Kapitel III nachzukommen.

(2) Aus eigenem Entschluss oder auf Antrag eines oder mehrerer Mitgliedstaaten, für den/die bzw. in dem/denen der wesentliche Dienst erbracht wird, und vorausgesetzt, der Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, stimmt dem zu, organisiert die Kommission eine Beratungsmission nach Absatz 1 des vorliegenden Artikels.

(3) Auf einen begründeten Antrag der Kommission oder eines oder mehrerer Mitgliedstaaten, für den/die bzw. in dem/denen der wesentliche Dienst erbracht wird, stellt der Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, der Kommission Folgendes zur Verfügung:

a) die entsprechenden Teile der Risikobewertung durch kritische Einrichtungen,

b) eine Auflistung der gemäß Artikel 13 ergriffenen entsprechenden Maßnahmen,

c) Aufsichts- oder Durchsetzungsmaßnahmen, die seine zuständige Behörde gemäß den Artikeln 21 und 22 in Bezug auf diese kritische Einrichtung ergriffen hat, einschließlich der Bewertungen der Einhaltung der Vorschriften oder der erteilten Anordnungen.

(4) Die Beratungsmission erstattet der Kommission, dem Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, den Mitgliedstaaten, für die bzw. in denen der wesentliche Dienst erbracht wird, und der betreffenden kritischen Einrichtung innerhalb von drei Monaten nach Abschluss der Beratungsmission über ihre Ergebnisse Bericht.

Die Mitgliedstaaten, für die bzw. in denen der wesentliche Dienst erbracht wird, analysieren den in Unterabsatz 1 genannten Bericht und beraten die Kommission erforderlichenfalls in Bezug auf die Frage, ob die betreffende kritische Einrichtung von besonderer Bedeutung für Europa ihre Verpflichtungen nach Kapitel III erfüllt, und gegebenenfalls hinsichtlich der Maßnahmen, die ergriffen werden könnten, um die Resilienz dieser kritischen Einrichtung zu verbessern.

Auf der Grundlage der Ratschläge gemäß Unterabsatz 2 dieses Absatzes teilt die Kommission dem Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, den Mitgliedstaaten, für die bzw. in denen der wesentliche Dienst erbracht wird, und der betreffenden kritischen Einrichtung ihre Stellungnahme zu der Frage, ob diese kritische Einrichtung ihre Verpflichtungen nach Kapitel III erfüllt, und gegebenenfalls hinsichtlich der Maßnahmen, die ergriffen werden könnten, um die Resilienz dieser kritischen Einrichtung zu verbessern, mit.

Der Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, stellt sicher, dass seine zuständige Behörde und die betreffende kritische Einrichtung der Stellungnahme gemäß Unterabsatz 3 dieses Absatzes gebührend Rechnung tragen, und unterrichtet die Kommission und die Mitgliedstaaten, für die bzw. in denen der wesentliche Dienst erbracht wird, über die Maßnahmen, die er aufgrund dieser Stellungnahme ergriffen hat.

(5) Jede Beratungsmission setzt sich aus Sachverständigen des Mitgliedstaats, in dem sich die kritische Einrichtung von besonderer Bedeutung für Europa befindet, aus Sachverständigen der Mitgliedstaaten, für die bzw. in denen der wesentliche Dienst erbracht wird, und Vertretern der Kommission zusammen. Diese Mitgliedstaaten können Kandidaten vorschlagen, die an einer Beratungsmission teilnehmen sollen. Die Kommission wählt nach Absprache mit dem Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat, die Mitglieder jeder Beratungsmission nach Maßgabe ihrer fachlichen Eignung und, soweit möglich, unter Gewährleistung einer geografisch ausgewogenen Vertretung aus allen diesen Mitgliedstaaten aus und ernennt sie. Erforderlichenfalls müssen die Mitglieder der Beratungsmission über eine gültige und angemessene Sicherheitsüberprüfung verfügen. Die Kommission trägt die Kosten im Zusammenhang mit der Teilnahme an Beratungsmissionen.

Die Kommission organisiert das Programm jeder Beratungsmission in Absprache mit den Mitgliedern der betreffenden Beratungsmission und im Einvernehmen mit dem Mitgliedstaat, der eine kritische Einrichtung von besonderer Bedeutung für Europa als kritische Einrichtung gemäß Artikel 6 Absatz 1 ermittelt hat.

(6) Die Kommission erlässt einen Durchführungsrechtsakt zur Festlegung von Vorschriften über die Verfahrensmodalitäten für Anträge zur Organisation der Beratungsmissionen, für die Bearbeitung solcher Anträge, für die Durchführung und die Berichterstattung von Beratungsmissionen sowie für die Handhabung der Mitteilung der in Absatz 4 Unterabsatz 3 des vorliegenden Artikels genannten Stellungnahme der Kommission und der ergriffenen Maßnahmen, wobei sie der Vertraulichkeit und der wirtschaftlichen Sensibilität der betreffenden Informationen gebührend Rechnung trägt. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 24 Absatz 2 genannten Prüfverfahren erlassen.

(7) Die Mitgliedstaaten stellen sicher, dass die kritischen Einrichtungen von besonderer Bedeutung für Europa den Beratungsmissionen Zugang zu Informationen, Systemen und Anlagen im Zusammenhang mit der Erbringung ihrer wesentlichen Dienste gewähren, die zur Durchführung der betreffenden Beratungsmission erforderlich sind.

(8) Beratungsmissionen werden im Einklang mit dem geltenden nationalen Recht des Mitgliedstaats, in dem sie stattfinden, durchgeführt, wobei die Verantwortung dieses Mitgliedstaats für die nationale Sicherheit und den Schutz seiner Sicherheitsinteressen zu achten ist.

(9) Bei der Organisation der Beratungsmissionen berücksichtigt die Kommission gegebenenfalls die Berichte über alle etwaigen Inspektionen gemäß den Verordnungen (EG) Nr. 725/2004 und (EG) Nr. 300/2008 sowie über jegliche Überwachung gemäß der Richtlinie 2005/65/EG, die die Kommission in Bezug auf die betreffende kritische Einrichtung durchgeführt hat.

(10) Die Kommission unterrichtet die gemäß Artikel 19 genannte Gruppe für die Resilienz kritischer Einrichtungen, wenn eine Beratungsmission organisiert wird. Der Mitgliedstaat, in dem die Beratungsmission durchgeführt wurde, und die Kommission unterrichten im Hinblick auf die Förderung gegenseitiger Lernprozesse die Gruppe für die Resilienz kritischer Einrichtungen auch über die wichtigsten Ergebnisse der Beratungsmission und die gewonnenen Erkenntnisse.

KAPITEL V

## ZUSAMMENARBEIT UND BERICHTERSTATTUNG

*Artikel 19*

### Gruppe für die Resilienz kritischer Einrichtungen

(1) Eine Gruppe für die Resilienz kritischer Einrichtungen wird hiermit eingesetzt. Die Gruppe für die Resilienz kritischer Einrichtungen unterstützt die Kommission und erleichtert die Zusammenarbeit zwischen den Mitgliedstaaten und den Informationsaustausch zu Fragen im Zusammenhang mit dieser Richtlinie.

(2) Die Gruppe für die Resilienz kritischer Einrichtungen setzt sich aus Vertretern der Mitgliedstaaten und der Kommission zusammen, die — soweit erforderlich — über eine Sicherheitsermächtigung verfügen. Wenn es für die Erfüllung ihrer Aufgaben relevant ist, kann die Gruppe für die Resilienz kritischer Einrichtungen entsprechende Interessenvertreter zur Teilnahme an ihrer Arbeit einladen. Wenn das Europäische Parlament darum ersucht, kann die Kommission Sachverständige des Europäischen Parlaments zur Teilnahme an den Sitzungen der Gruppe für die Resilienz kritischer Einrichtungen einladen.

Der Vertreter der Kommission führt den Vorsitz der Gruppe für die Resilienz kritischer Einrichtungen.

(3) Die Gruppe für die Resilienz kritischer Einrichtungen hat folgende Aufgaben:

a) Unterstützung der Kommission bei der Unterstützung der Mitgliedstaaten beim Ausbau ihrer Kapazitäten im Hinblick auf die Gewährleistung der Resilienz kritischer Einrichtungen im Einklang mit dieser Richtlinie;

b) Analyse der Strategien zur Ermittlung bewährter Verfahren bezüglich dieser Strategien;

c) Erleichterung des Austauschs bewährter Verfahren in Bezug auf die Ermittlung kritischer Einrichtungen durch die Mitgliedstaaten gemäß Artikel 6 Absatz 1, auch im Zusammenhang mit grenzüberschreitenden und sektorübergreifenden Abhängigkeiten und im Hinblick auf Risiken und Sicherheitsvorfälle;

d) gegebenenfalls Mitwirkung — in Bezug auf Fragen im Zusammenhang mit dieser Richtlinie — an Dokumenten über die Resilienz auf Unionsebene;

e) Mitwirkung an der Ausarbeitung der in Artikel 7 Absatz 3 und Artikel 13 Absatz 5 genannten Leitlinien und — auf Ersuchen — aller delegierten Rechtsakte oder Durchführungsrechtsakte, die im Rahmen dieser Richtlinie angenommen wurden;

f) Analyse der in Artikel 9 Absatz 3 genannten zusammenfassenden Berichte mit dem Ziel, den Austausch bewährter Verfahren für die gemäß Artikel 15 Absatz 3 ergriffenen Maßnahmen zu fördern;

g) Austausch von bewährten Verfahren im Zusammenhang mit der Meldung von Sicherheitsvorfällen gemäß Artikel 15;

h) Erörterung der zusammenfassenden Berichte der Beratungsmissionen und der Erkenntnisse gemäß Artikel 18 Absatz 10;

i) Austausch von Informationen und bewährten Verfahren hinsichtlich Innovation, Forschung und Entwicklung im Zusammenhang mit der Resilienz kritischer Einrichtungen gemäß dieser Richtlinie;

j) gegebenenfalls Informationsaustausch zu Fragen, die die Resilienz kritischer Einrichtungen betreffen, mit den entsprechenden Organen, Einrichtungen und sonstigen Stellen der Union.

(4) Bis zum 17. Januar 2025 und danach alle zwei Jahre erstellt die Gruppe für die Resilienz kritischer Einrichtungen ein Arbeitsprogramm mit den Maßnahmen, die zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen sind. Dieses Arbeitsprogramm steht im Einklang mit den Anforderungen und Zielen dieser Richtlinie.

(5) Die Gruppe für die Resilienz kritischer Einrichtungen tagt regelmäßig und in jedem Fall mindestens einmal jährlich gemeinsam mit der durch die Richtlinie (EU) 2022/2555 eingerichteten Kooperationsgruppe, um die Zusammenarbeit und den Informationsaustausch zu fördern und zu erleichtern.

(6) Die Kommission kann unter Beachtung von Artikel 1 Absatz 4 Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten, die für das Funktionieren der Gruppe für die Resilienz kritischer Einrichtungen erforderlich sind, erlassen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 24 Absatz 2 genannten Prüfverfahren erlassen.

(7) Die Kommission übermittelt der Gruppe für die Resilienz kritischer Einrichtungen bis zum 17. Januar 2027 und anschließend im Bedarfsfall, mindestens jedoch alle vier Jahre, einen zusammenfassenden Bericht über die von den Mitgliedstaaten gemäß Artikel 4 Absatz 3 und Artikel 5 Absatz 4 übermittelten Informationen.

*Artikel 20*

**Unterstützung der zuständigen Behörden und kritischen Einrichtungen durch die Kommission**

(1) Die Kommission unterstützt die Mitgliedstaaten und die kritischen Einrichtungen gegebenenfalls bei der Erfüllung ihrer Verpflichtungen gemäß dieser Richtlinie. Die Kommission erstellt eine unionsweite Übersicht über grenzüberschreitende und sektorübergreifende Risiken für die Erbringung wesentlicher Dienste, organisiert die in Artikel 13 Absatz 4 und Artikel 18 genannten Beratungsmissionen und erleichtert den Informationsaustausch zwischen Mitgliedstaaten und Sachverständigen in der gesamten Union.

(2) Die Kommission ergänzt die in Artikel 10 genannten Tätigkeiten der Mitgliedstaaten, indem sie bewährte Verfahren, Leitfäden und Methoden ausarbeitet und grenzüberschreitende Schulungsmaßnahmen und grenzüberschreitende Übungen zur Überprüfung der Resilienz kritischer Einrichtungen entwickelt.

(3) Die Kommission unterrichtet die Mitgliedstaaten über die finanziellen Ressourcen auf Unionsebene, die den Mitgliedstaaten zur Verbesserung der Resilienz kritischer Einrichtungen zur Verfügung stehen.

KAPITEL VI

**AUFSICHT UND DURCHSETZUNG**

*Artikel 21*

**Aufsicht und Durchsetzung**

(1) Im Hinblick auf die Beurteilung, ob die Einrichtungen, die die Mitgliedstaaten gemäß Artikel 6 Absatz 1 als kritische Einrichtungen eingestuft haben, die in dieser Richtlinie festgelegten Verpflichtungen erfüllen, stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, um

a) Vor-Ort-Kontrollen der kritischen Infrastruktur und der Räumlichkeiten, die die kritische Einrichtung für die Erbringung ihrer wesentlichen Dienste nutzt, und externe Aufsichtsmaßnahmen bezüglich der von kritischen Einrichtungen ergriffenen Maßnahmen gemäß Artikel 13 durchzuführen;

b) Audits bei kritischen Einrichtungen durchzuführen oder anzuordnen.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden über die Befugnisse und Mittel verfügen, von den Einrichtungen gemäß der Richtlinie (EU) 2022/2555, die die Mitgliedstaaten gemäß dieser Richtlinie als kritische Einrichtungen eingestuft haben, — wenn dies für die Wahrnehmung ihrer Aufgaben gemäß dieser Richtlinie erforderlich ist — zu verlangen, dass sie innerhalb einer von diesen Behörden festgelegten angemessenen Frist Folgendes übermitteln:

a) die Informationen, die erforderlich sind, um beurteilen zu können, ob die Maßnahmen, die diese Einrichtungen zur Gewährleistung ihrer Resilienz ergriffen haben, die Anforderungen gemäß Artikel 13 erfüllen;

b) Nachweise der wirksamen Umsetzung dieser Maßnahmen, einschließlich der Ergebnisse eines Audits, das von einem unabhängigen und qualifizierten von der betreffenden Einrichtung ausgewählten Prüfer auf Kosten der betreffenden Einrichtung durchgeführt wurde.

Bei der Anforderung dieser Informationen nennen die zuständigen Behörden den Zweck und geben an, welche Informationen verlangt werden.

(3) Unbeschadet der Möglichkeit, Sanktionen gemäß Artikel 22 zu verhängen, können die zuständigen Behörden im Anschluss an die in Absatz 1 des vorliegenden Artikels genannten Aufsichtsmaßnahmen oder die Prüfung der in Absatz 2 des vorliegenden Artikels genannten Informationen die betreffenden kritischen Einrichtungen anweisen, erforderliche und verhältnismäßige Maßnahmen zu ergreifen, um festgestellte Verstöße gegen diese Richtlinie innerhalb einer von diesen Behörden gesetzten angemessenen Frist zu beheben, und diesen Behörden Informationen über die ergriffenen Maßnahmen zu übermitteln. Diese Anweisungen tragen insbesondere der Schwere des Verstoßes Rechnung.

(4) Die Mitgliedstaaten stellen sicher, dass die in den Absätzen 1, 2 und 3 vorgesehenen Befugnisse nur vorbehaltlich angemessener Garantien ausgeübt werden können. Diese Garantien gewährleisten insbesondere, dass die Befugnisse auf objektive, transparente und verhältnismäßige Weise ausgeübt werden und dass die Rechte und berechtigten Interessen der betreffenden kritischen Einrichtungen — wie der Schutz von Handels- und Geschäftsgeheimnissen — ordnungsgemäß gewahrt werden, einschließlich ihres Rechts auf Anhörung, Verteidigung und eines wirksamen Rechtsbehelfs vor einem unabhängigen Gericht.

(5) Die Mitgliedstaaten stellen sicher, dass eine nach dieser Richtlinie zuständige Behörde, wenn sie die Erfüllung der Verpflichtungen einer kritischen Einrichtung gemäß diesem Artikel bewertet, dies den gemäß der Richtlinie (EU) 2022/2555 zuständigen Behörden der betreffenden Mitgliedstaaten mitteilt. Zu diesem Zweck stellen die Mitgliedstaaten sicher, dass nach dieser Richtlinie zuständige Behörden die zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 ersuchen können, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine in den Anwendungsbereich dieser Richtlinie fallende Einrichtung auszuüben, die gemäß der vorliegenden Richtlinie als kritische Einrichtung eingestuft wurde. Zu diesem Zweck stellen die Mitgliedstaaten sicher, dass die nach dieser Richtlinie zuständigen Behörden mit den zuständigen Behörden gemäß der Richtlinie (EU) 2022/2555 zusammenarbeiten und Informationen austauschen.

*Artikel 22*

**Sanktionen**

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Vorschriften zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 17. Oktober 2024 mit und melden ihr umgehend etwaige spätere diesbezügliche Änderungen.

KAPITEL VII

**DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE**

*Artikel 23*

**Ausübung der Befugnisübertragung**

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 5 Absatz 1 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 16. Januar 2023 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 5 Absatz 1 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 5 Absatz 1 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

*Artikel 24*

**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.

KAPITEL VIII

**SCHLUSSBESTIMMUNGEN**

*Artikel 25*

**Berichterstattung und Überprüfung**

Die Kommission übermittelt dem Europäischen Parlament und dem Rat bis zum 17. Juli 2027 einen Bericht, in dem sie bewertet, inwieweit jeder Mitgliedstaat die erforderlichen Maßnahmen getroffen hat, um dieser Richtlinie nachzukommen.

Die Kommission überprüft regelmäßig die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In diesem Bericht werden insbesondere der Mehrwert dieser Richtlinie, ihre Auswirkungen auf die Gewährleistung der Resilienz kritischer Einrichtungen beurteilt und geprüft, und ob der Anhang dieser Richtlinie geändert werden sollte. Die Kommission legt den ersten dieser Berichte bis zum 17. Juni 2029 vor Für die Zwecke der Berichterstattung gemäß dieses Artikels berücksichtigt die Kommission entsprechende Dokumente der Gruppe für die Resilienz kritischer Einrichtungen.

*Artikel 26*

**Umsetzung**

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

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

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

*Artikel 27*

**Aufhebung der Richtlinie 2008/114/EG**

Die Richtlinie 2008/114/EG wird mit Wirkung vom 18. Oktober 2024 aufgehoben.

Bezugnahmen auf die aufgehobene Richtlinie gelten als Bezugnahmen auf die vorliegende Richtlinie.

*Artikel 28*

**Inkrafttreten**

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

*Artikel 29*

**Adressaten**

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

Geschehen zu Straßburg am 14. Dezember 2022.

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

*ANHANG*

**SEKTOREN, TEILSEKTOREN UND KATEGORIEN VON EINRICHTUNGEN**

| Sektoren | Teilsektoren | Kategorien von Einrichtungen |
|---|---|---|
| 1. Energie | a) Strom | — Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates ([1]), die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen |
| | | — Verteilernetzbetreiber im Sinne 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 des Europäischen Parlaments und des Rates ([2]) |
| | | — Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten |
| | b) Fernwärme und -kälte | — Betreiber von Fernwärme- oder -kälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates ([3]) |
| | c) Erdöl | — Betreiber von Erdöl-Fernleitungen |
| | | — Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie von Erdöllagern und Erdöl-Fernleitungen |
| | | — Zentrale Bevorratungsstellen im Sinne des Artikels 2 Buchstabe f der Richtlinie 2009/119/EG des Rates ([4]) |

| Sektoren | Teilsektoren | Kategorien von Einrichtungen |
|---|---|---|
| | d) Erdgas | — Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates ([5]) |
| | | — Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG |
| | | — Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/73/EG |
| | | — Betreiber einer Speicheranlage im Sinne des Artikels 2 Nummer 10 der Richtlinie 2009/73/EG |
| | | — Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG |
| | | — Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG |
| | | — Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas |
| | e) Wasserstoff | — Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung |
| 2. Verkehr | a) Luftfahrt | — Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden |
| | | — Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates ([6]), Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates ([7]) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben |
| | | — Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates ([8]) bereitstellen |

| Sektoren | Teilsektoren | Kategorien von Einrichtungen |
|---|---|---|
| | b) Schienenverkehr | — Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates ([9]) |
| | | — Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU und Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 jener Richtlinie |
| | c) Schifffahrt | — Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe |
| | | — Leitungsorgane von Häfen im Sinne des Artikels 3 Absatz 1 der Richtlinie 2005/65/EG, einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben |
| | | — Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates ([10]) |
| | d) Straßenverkehr | — Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission ([11]), die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist |
| | | — Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates ([12]) |
| | e) Öffentlicher Verkehr | — Betreiber eines öffentlichen Dienstes im Sinne des Artikels 2 Buchstabe d der Verordnung (EG) Nr. 1370/2007 des Europäischen Parlaments und des Rates ([13]) |
| 3. Bankwesen | | — Kreditinstitute im Sinne des Artikels 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 |
| 4. Finanzmarktinfrastrukturen | | — Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU |
| | | — Zentrale Gegenparteien (CCP) im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 |

| Sektoren | Teilsektoren | Kategorien von Einrichtungen |
|---|---|---|
| 5. Gesundheit | | — Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates ([14]) |
| | | — EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates ([15]) |
| | | — Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates ([16]) ausüben |
| | | — Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen |
| | | — Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates ([17]) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden |
| | | — Einrichtungen, die eine Großhandelsgenehmigung im Sinne des Artikels 79 der Richtlinie 2001/83/EG besitzen |
| 6. Trinkwasser | | — Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates ([18]), unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist |
| 7. Abwasser | | — Unternehmen, die kommunales, häusliches oder industrielles Abwasser im Sinne des Artikels 2 Nummern 1 bis 3 der Richtlinie 91/271/EWG des Rates ([19]) sammeln, entsorgen oder behandeln, unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist |

| Sektoren | Teilsektoren | Kategorien von Einrichtungen |
|---|---|---|
| 8. Digitale Infrastruktur | | — Betreiber von Internet-Knoten im Sinne des Artikels 6 Nummer 18 der Richtlinie (EU) 2022/2555 |
| | | — DNS-Diensteanbieter im Sinne des Artikels 6 Nummer 20 der Richtlinie (EU) 2022/2555, ausgenommen Betreiber von Root-Namenservern |
| | | — TLD-Namenregister im Sinne des Artikels 6 Nummer 21 der Richtlinie (EU) 2022/2555 |
| | | — Anbieter von Cloud-Computing-Diensten im Sinne des Artikels 6 Nummer 30 der Richtlinie (EU) 2022/2555 |
| | | — Anbieter von Rechenzentrumsdiensten im Sinne des Artikels 6 Nummer 31 der Richtlinie (EU) 2022/2555 |
| | | — Betreiber von Inhaltszustellnetzen im Sinne des Artikels 6 Nummer 32 der Richtlinie (EU) 2022/2555 |
| | | — Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([20]) |
| | | — Anbieter öffentlicher elektronischer Kommunikationsnetze im Sinne des Artikels 2 Nummer 8 der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([21]) |
| | | — Anbieter elektronischer Kommunikationsdienste im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972, soweit deren Dienste öffentlich zugänglich sind |
| 9. Öffentliche Verwaltung | | — Einrichtungen der öffentlichen Verwaltung von Zentralregierungen entsprechend der jeweiligen Definition der Mitgliedstaaten gemäß nationalem Recht |
| 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 |

| Sektoren | Teilsektoren | Kategorien von Einrichtungen |
|---|---|---|
| 11. Produktion, Verarbeitung und Vertrieb von Lebensmitteln | | — Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates ([22]), die ausschließlich Logistik und Großhandel sowie industrielle Großproduktion und -verarbeitung betreiben |

([1]) Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU (ABl. L 158 vom 14.6.2019, S. 125).

([2]) Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54).

([3]) Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen (ABl. L 328 vom 21.12.2018, S. 82).

([4]) Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten (ABl. L 265 vom 9.10.2009, S. 9).

([5]) Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt und zur Aufhebung der Richtlinie 2003/55/EG (ABl. L 211 vom 14.8.2009, S. 94).

([6]) Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11).

([7]) Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348 vom 20.12.2013, S. 1).

([8]) Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums („Rahmenverordnung“) (ABl. L 96 vom 31.3.2004, S. 1).

([9]) Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates vom 21. November 2012 zur Schaffung eines einheitlichen europäischen Eisenbahnraums (ABl. L 343 vom 14.12.2012, S. 32).

([10]) 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).

([11]) 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).

([12]) 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).

([13]) Verordnung (EG) Nr. 1370/2007 des Europäischen Parlaments und des Rates vom 23. Oktober 2007 über öffentliche Personenverkehrsdienste auf Schiene und Straße und zur Aufhebung der Verordnungen (EWG) Nr. 1191/69 und (EWG) Nr. 1107/70 des Rates (ABl. L 315 vom 3.12.2007, S. 1).

([14]) 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).

([15]) Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26).

([16]) 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).

([17]) Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1).

([18]) Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates vom 16. Dezember 2020 über die Qualität von Wasser für den menschlichen Gebrauch (ABl. L 435 vom 23.12.2020, S. 1).

([19]) 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).

([20]) 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).

([21]) 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).

([22]) 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).

ISSN 1977-0642 (elektronische Ausgabe)
ISSN 1725-2539 (Papierausgabe)

Amt für Veröffentlichungen
der Europäischen Union
L-2985 Luxemburg
LUXEMBURG

DE